Exploiting Radio Channel Aware Physical Layer Concepts

Deutscher Titel:

Zur Nutzung von Kanalzustandsinformation in Funkübertragungskonzepten

vom

Fachbereich Elektrotechnik und Informationstechnik der Technischen Universität Kaiserslautern zur Verleihung des akademischen Grades

Doktor der Ingenieurwissenschaften (Dr.-Ing.)

genehmigte Dissertation

von

Abhijit Ambekar, M.Tech.
geb. in Hubli, Karnataka, (India)

D386

Eingereicht am:	06. Mai 2015
Tag der mündlichen Prüfung:	05. Oktober 2015
Dekan des Fachbereichs:	Prof. Dr.-Ing. Hans D. Schotten
Promotionskommission:	
Vorsitzender:	Prof. Dr.-Ing. Ralph Urbansky
Berichterstattende:	Prof. Dr.-Ing. Hans D. Schotten
	Prof. Dr.-Ing. Aydin Sezgin

Contents

List of Figures

List of Tables

Dedicated to Guruji

ACKNOWLEDGEMENTS

I express my gratitude to my supervisor Prof. Dr.-Ing. Hans D. Schotten for giving me an opportunity to pursue my PhD under his supervision. I thank him for all the scientific guidance and discussions I had with him over the years. I am also grateful to Prof.Schotten for the PhD scholarship that was granted to me for the period of four and half years, and for giving me the opportunity to work in the project *Prophylaxe*.

I sincerely thank Prof. Dr.-Ing. Aydin Sezgin from the Rühr Universität Bochum for being my second supervisor. I thank Prof. Aydin for giving me an opportunity to present my work in Bochum and for giving scientific advise and suggestions regarding my thesis.

I thank all the members of my research group for the wonderful discussions and good time we had over the years. I thank all my collaborators especially from the Project Prophylaxe for the scientific discussions and suggestions.

My family and friends played a big role in providing with a great support system during my PhD. I am very grateful to all of you. Last but not the least, I thank my wife Kavya who supported me through my thick and thin, putting aside her own goals all for my dreams.

Abstrakt

In DS-CDMA Verfahren werden Nutzern eindeutige Spreizcodes zugeordnet, um ihre Signale unterscheiden zu können. Dieses Verfahren wird sowohl in der Downlink Richtung von der Basisstation zum Nutzer und als auch in der Uplink-Richtung vom Nutzer zur Basisstation eingesetzt. Spreizcodes werden in der Regel unter Berücksichtigung ihrer periodischen Korrelationseigenschaften entworfen. Spreizcodes mit guten Autokorrelationseigenschaften helfen dem Empfänger Datenrahmen zu synchronisieren, während periodische Spreizcodes mit gutem Kreuzkorrelationseigenschaften das Übersprechen zwischen Nutzern und dadurch gegenseitige Störungen reduzieren. Weiterhin sind für viele dieser Spreizcodes effiziente Implementierungskonzepte bekannt. In heutigen Systemen erfolgt die Zuordnung der Spreizcodes zu den Nutzern unabhängig vom jeweiligen Kanalzustand. In dieser Arbeit wird die Methode der kanalzustandsabhängigen Zuordnung von Spreizcodes untersucht, um das Leistungsvermögen des Downlinks zu verbessern. Verschiedene Methoden der dynamischen Zuordnung der Codes werden evaluiert, unter anderem die optimale Allokation, eine schnelle suboptimale Allokation durch ein mathematisches Modell und ein Proof-of-Concept-Modell mit Echtzeitkanalmessungen.

In der Kryptographie werden geheime Schlüssel verwendet, um die Vertraulichkeit der Kommunikation zwischen Netzwerknoten zu gewährleisten. Die Übertragungsart in einem drahtlosen Ad-hoc- Netzwerk verlangt ein robustes Schlüssel verwaltungssystem. Sicherheit in der physikalischen Schicht ist ein neuer Ansatz, der die zufällig wirkenden Schwankungen des Kanals und die Kanalreziprozität zur Schlüsselerzeugung verwendet. Durch den reziproken Charakter des drahtlosen Kanals kann ein gemeinsamer Schlüssel zwischen einem Knotenpaar erzeugt werden. Der Prozess der Schlüsselextraktion besteht aus den folgenden vier Schritten: Kanalmessung, Quantisierung, ”Information Reconciliation”, und ”Privacy Amplification”. Die reziproken Kanalschwankungen werden gemessen und quan-

tisiert, um einen vorläufigen Schlüssel aus Bit-Vektoren zu erhalten. Aufgrund von Mess-und Quantisierungsfehlern, sowie Gaußschem Rauschen bestehen zunächst Unstimmigkeiten zwischen den vorläufigen Schlüsseln. Mit Hilfe von Fehlererkennungs und Fehlerkorrekturmaßnahmen werden diese korrigiert und das Knotenpaar erhält einen synchronisierten Schlüssel. Des Weiteren wird durch die Methode des sicheren Hashings die Entropie des Schlüssels in der "Privacy Amplification" Phase erhöht. Die Effizienz des Schlüsselgenerierungsprozesses hängt von der Kanalmessmethode und dem Quantisierungsverfahren ab. Anstatt die Kanalmessung direkt zu quantisieren, wird der reziproke Wert verstärkt und entsprechend quantisiert, um die Schlüsselgenerierung effizienter und schneller zu machen. In dieser Arbeit werden vier Methoden zur Verstärkung der Reziprozität vorgestellt: l_1-Norm Minimierung, Gruppierung durch hierarchisches Clustern, Kalman Filterung, und polynomiale Regression. Diese werden entsprechend binär und adaptiv quantisiert. Danach wird der gesamte Schlüsselerzeugungsprozess, von der Kanalprofilmessung bis zum Erhalten des Schlüssels, durch Echtzeit kanalmessungen validiert. Die Performanzevaluierung erfolgt durch den Vergleich von Bitfehlerrate und Schlüsselgenerierungsraten, Zufälligkeitstests, Robustheitstests und Abhörtests. Eine Architektur, KeyBunch, wird vorgeschlagen, um die Sicherheit der physikalischen Schicht effizient in mobilen ad-hoc Netzwerken und Ad-hoc-Netzwerken in Fahrzeugen einzubinden. Schließlich wird KeyBunch als Anwendungsfall in einer sicheren Fahrzeug Kommunikationsarchitektur eingebunden, um die Vorteile der Sicherheit in der physikalischen Sicht hervorzuheben.

Abstract

In DS-CDMA, spreading sequences are allocated to users to separate different links namely, the base-station to user in the downlink or the user to base station in the uplink. These sequences are designed for optimum periodic correlation properties. Sequences with good periodic auto-correlation properties help in frame synchronisation at the receiver while sequences with good periodic cross-correlation property reduce cross-talk among users and hence reduce the interference among them. In addition, they are designed to have reduced implementation complexity so that they are easy to generate. In current systems, spreading sequences are allocated to users irrespective of their channel condition. In this thesis, the method of allocating spreading sequences based on users' channel condition is investigated in order to improve the performance of the downlink. Different methods of dynamically allocating the sequences are investigated including; optimum allocation through a simulation model, fast sub-optimum allocation through a mathematical model, and a proof-of-concept model using real-world channel measurements. Each model is evaluated to validate, improvements in the gain achieved per link, computational complexity of the allocation scheme, and its impact on the capacity of the network.

In cryptography, secret keys are used to ensure confidentiality of communication between the legitimate nodes of a network. In a wireless ad-hoc network, the broadcast nature of the channel necessitates robust key management systems for secure functioning of the network. *Physical layer security* is a novel method of profitably utilising the random and reciprocal variations of the wireless channel to extract secret key. By measuring the characteristics of the wireless channel within its coherence time, reciprocal variations of the channel can be observed between a pair of nodes. Using these reciprocal characteristics of the wireless channel, a

common shared secret key is extracted between a pair of the nodes. The process of key extraction consists of four steps namely; channel measurement, quantisation, information reconciliation, and privacy amplification. The reciprocal channel variations are measured and quantised to obtain a preliminary key of vector bits $(0, 1)$. Due to errors in measurement, quantisation, and additive Gaussian noise, disagreement in the bits of preliminary keys exists. These errors are corrected by using, error detection and correction methods to obtain a synchronised key at both the nodes. Further, by the method of secure hashing, the entropy of the key is enhanced in the privacy amplification stage. The efficiency of the key generation process depends on the method of channel measurement and quantisation. Instead of quantising the channel measurements directly, if their reciprocity is enhanced and then quantised appropriately, the key generation process can be made efficient and fast. In this thesis, four methods of enhancing reciprocity are presented namely; l_1-norm minimisation, Hierarchical clustering, Kalman filtering, and Polynomial regression. They are appropriately quantised by binary and adaptive quantisation. Then, the entire process of key generation, from measuring the channel profile to obtaining a secure key is validated by using real-world channel measurements. The performance evaluation is done by comparing their performance in terms of bit disagreement rate, key generation rate, test of randomness, robustness test, and eavesdropper test. An architecture, *KeyBunch*, for effectively deploying the physical layer security in mobile and vehicular ad-hoc networks is also proposed. Finally, as an use-case, KeyBunch is deployed in a secure vehicular communication architecture, to highlight the advantages offered by physical layer security.

Chapter 1

Introduction

In my thesis, I have focused on two topics namely; *channel aware adaptation of spreading sequences* and *physical layer security*. In the first topic, I investigate the method of allocating spreading sequences to users of direct sequence code division multiple access (DS-CDMA) system, based on their channel condition. While in the second topic, I investigate the method of extracting shared secret keys using the reciprocal variations of the wireless channel.

DS-CDMA uses spreading sequences to separate different links, e.g., the base-station to user links in the downlink or the user to base-station links in the up-link. These sequences are usually allocated when the link is set up and kept fixed for the duration of the transmission. They are mainly designed to have good auto-correlation and cross-correlation properties. Good auto-correlation properties help in frame synchronisation at the receiver. While sequences with good cross-correlation properties help in reduced cross-talk and interference between different simultaneous DS-CDMA links. Generally sequences with good correlation properties are allocated to users of DS-CDMA system irrespective of their channel condition. In this thesis, the principle concept of allocating optimum sequences based on users' channel condition is investigated.

In cryptography, the main attributes of a secure network are defined to include; *availability*, *confidentiality*, *integrity*, *authentication*, and *non-repudiation*

of the nodes. Secret keys are necessary to maintain the confidentiality of communication between the legitimate nodes of a network. Traditionally secret keys are established between the legitimate nodes using symmetric or asymmetric method of cryptography. Hershey et.al. first introduced the concept of physical layer security in 1995 [44]. They showed that by exploiting the random and reciprocal characteristics of the wireless channel, shared secret keys could be established between a pair of nodes in the wireless network. With the advent of Internet-of-things (IoTs), wherein energy constrained devices are all inter-connected to form an ad-hoc network, security of IoT based devices has become very important. As the IoT based devices are energy constrained and have limitations on their computational resources, the traditional method of key management using asymmetric or symmetric key cryptography is not very effective. In such cases, physical layer security offers a new paradigm of profitably exploiting the wireless channel to effectively establish shared secret keys. In this thesis, methods of effectively establishing physical layer security for devices in IoT are investigated.

1.1 Problem Statement

1. **Channel aware adaptation of spreading sequences**: To develop resource allocation algorithms for allocating sequences to users based on their channel condition. The proposed algorithms must be evaluated for their performance in terms of gain achieved per link, computational complexity of allocation, and the effect on network capacity.

2. **Physical layer security**: To build effective secret key management systems using the reciprocal variations of the wireless channel. It includes reciprocity enhancement methods and appropriate quantisation methods. The proposed key management methods are to be validated on testbeds that yield real-world channel measurements. Further, architectures and frameworks for deploying the key management systems in stationary, mobile, and vehicular ad-hoc networks are investigated.

1.2 Contributions of the Thesis

1.2.1 Channel aware adaptation of spreading sequences

Using different models such as; simulation model, analytical model, and hardware model, the allocation of spreading sequences based on users' channel condition is investigated.

1. Simulation model: In the simulation model, I have proposed an optimum method of allocation based on the Hungarian algorithm. This method allows an optimum allocation of spreading sequences to users based on their channel properties. Further, evaluation of its performance in terms of gain achieved per link and the computational complexity of the allocation scheme has also been done. The results of this model have been published in [8, 9].

2. Analytical model: In the analytical model, an expectation of the achievable gain for optimum allocation is calculated. To compensate for the overhead of computational complexity, a fast sub-optimal allocation method is proposed. The results of this model have been published in [9, 21].

3. Hardware model: As a proof-of-concept, channel co-efficients from real world are measured using a software defined radio platform. The measurements are then used to validate the concept of adaptation of sequences based on simulation and analytical model. The results of this model are under submission.

1.2.2 Physical layer security

The main contributions of my thesis in physical layer security are:

1. Enhancing channel reciprocity: To improve the efficiency of quantisation, I have investigated different methods of enhancing channel reciprocity namely:

   (a) l_1-norm minimisation

(b) Hierarchical clustering

(c) Kalman filtering

(d) Polynomial regression

These methods have been evaluated with real-world channel measurements to validate improvement in the performance. The results have been published in [5, 4, 10].

2. Quantisation: In order to generate preliminary keys from channel profiles, two quantisation methods, *median* and *adaptive quantisation* have been proposed. These methods were evaluated with real-world channel measurements and have been published in [5, 4, 10].

3. PhySec framework: A complete framework for physical layer security starting from initial channel measurement, enhancing channel reciprocity, quantisation, information reconciliation, and privacy amplification has been presented in my thesis.

4. Cross-layered architecture: By combining the traditional method of asymmetric cryptography and physical layer security, a cross-layered approach of key management for resource constrained platforms has been presented in [104]. This was a joint work with the security group EMSEC at the Ruhr University Bochum.

5. KeyBunch: A key management architecture to effectively generate and distribute secret keys using various channel profiles and quantisation schemes is presented.

6. Evaluation and validation: The proposed framework has been evaluated using real world channel measurements. The measurements include three types of wireless channel namely:

(a) Indoor static channel: 2x3 MIMO measurements provided by Fraunhofer HHI Berlin have been used to validate the effect and importance of frequency selectivity in static environments. The results of this work are currently under submission.

(b) Outdoor mobile channel: Measurements from mobile ad-hoc network derived using wireless cards have been used to validate the physical layer security framework. The results of this work have been published in [5, 4, 10].

(c) Outdoor vehicular channel: As a test case for car-to-car communication, measurements from vehicular channel have been used and validated. The results of this work have been published in [5, 4, 10].

7. Finally a real-time USRP based demo, showing the extraction of secret keys based on RSSI has been evaluated.

The contributions of the thesis have been published in various peer reviewed conferences. The publication list for channel aware adaptation of spreading sequences are [8, 9, 21]. While the publication list for physical layer security are [5, 4, 10, 104]. While publications [6, 7] are under submission.

1.3 Organisation of the Thesis

The organisation of the thesis is as follows:

1. An introduction to DS-CDMA, link adaptation, and design of spreading sequences is presented in Chapter 2.

2. In Chapter 3, the principle concept of channel aware adaptation of spreading sequences is discussed. With the help of a link model and system model, the principle concept of dynamically allocating the spreading sequences is presented. The different methods of modeling namely; simulation model, analytical model, and hardware model are also investigated.

3. The state of the art of physical layer security is presented in Chapter 4. It includes a broad overview of the need for security in wireless ad-hoc networks and the principle of channel reciprocity. Then the standard method of key generation in physical layer security is presented. Further, the evaluation metrics used to validate the methods and the need for better methods of key generation are discussed.

4. In Chapter 5, different methods of channel reciprocity enhancement, quantisation, information reconciliation, and privacy amplification are investigated. An architecture to employ physical layer security in wireless ad-hoc networks is also proposed. Finally, an use-case for deploying physical layer security based key management system in vehicular communication is presented.

5. Chapter 6 deals with the testbed used to obtain real-world channel measurements and to validate the key generation algorithms. Further, the performance of the key generation algorithms are evaluated and their results are compared with those present in the state of art.

6. Finally, the main contributions of the thesis are concluded in Chapter 7. Further directions for future work are also outlined.

Chapter 2

Link Adaptation in DS-CDMA

The wireless channel is the medium of data transmission in wireless communication. Its main characteristic being variations of the channel strength over time and frequency [90]. These variations lead to large-scale and small-scale fading of the transmitted signal. Large-scale fading is frequency independent and results in path loss and shadowing. While small-scale fading is frequency dependent and leads to multi-path interference. Typically, transmitter-receiver systems are built around the characteristics of the channel in order to maximize the system performance and to deliver a required quality-of-service (QoS).

2.1 Direct Sequence Code Division Multiple Access

Direct sequence code division multiple access (DS-CDMA) is an access scheme that allows users to access the channel at the same time and frequency. Unlike time division duplex (TDD) and frequency division duplex (FDD) schemes, users transmit asynchronously in DS-CDMA as there is no need for precise time or frequency co-ordination. Wideband code division multiple access (WCDMA) is an air interface standard that uses DS-CDMA channel access method in Third generation mobile communication (3G). It is expected that by the end of 2018, WCDMA will be supporting up to 4.4 Billion subscribers worldwide [1].

In DS-CDMA, the information signal is spread to a higher bandwidth by modulating it with a spreading sequence. Spreading sequences are variations of predefined set of alphabets. They are constructed for optimum correlation properties. Sequences with good correlation properties either periodic or aperiodic, enhance system performance. For instance, sequences that satisfy the orthogonal property or the Welch bound on the total squared correlation with equality, maximise the information theoretic capacity for a single cell synchronous single path DS-CDMA. DS-CDMA uses spreading sequences to separate different links, e.g., the base-station to user links in the downlink or the user to base-station links in the uplink. These sequences are usually allocated when the link is set up and kept fixed for the duration of the transmission. They are mainly designed to have good cross-correlation properties in order to avoid interference and to be easy to generate in order to reduce the implementation complexity. In addition, they are designed to have good auto-correlation properties or equivalently a flat spectrum since this guarantees the anti-fading capability of DS-CDMA links.

2.1.1 Properties of Sequences

Spreading sequences are designed for various properties such as:

1. Period(N): The number of elements present in a single set of a sequence is known as period of a sequence. It basically determines the length of the sequence.

2. Family size(M): It is the number of sequence sets in a family of sequence.

3. Correlation($R_{i,i}(\tau), R_{i,j}(\tau)$): Correlation of a pair of sequence is, the measure of the degree of similarity between them. If the measure of similarity is between a sequence $\hat{a}_n(i)$ and its time shifted version $\hat{a}_n(i+\tau)$, then it is known as *auto-correlation ($R_{i,i}(\tau)$) where:*

$$R_{i,i}(\tau) = \sum_{n=0}^{N-1} a_n(i)(\hat{a}_n(i+\tau))^* \tag{2.1}$$

While if the measure of similarity is between two different sets of sequences $\hat{a}_n(i)$ *and* $\hat{b}_n(i)$*, then it is known as* cross-correlation ($R_{i,j}(\tau)$) where:

$$R_{i,j}(\tau) = \sum_{n=0}^{N-1} a_n(i)(\hat{b}_n(j+\tau))^* \tag{2.2}$$

4. Maximum Non-trivial Correlation(R_{max}): The maximum non-trivial correlation is defined as

$$R_{max} = max\{R_{am}, R_{cm}\} \tag{2.3}$$

where R_{am} is the maximum out-of-phase(side-lobes) auto-correlation value and R_{cm} is the maximum out-of-phase cross-correlation value.

5. Based on the maximum non-trivial correlation values, different sets of bounds have been proposed namely:

   (a) Sarwate bound [83]

$$\frac{R_{cm}^2}{N} + \frac{N-1}{N(M-1)}\frac{R_{am}^2}{N} \geq 1 \tag{2.4}$$

   (b) Welch bound [96]

$$R_{max} \geq N\sqrt{\frac{M-1}{NM-1}} \tag{2.5}$$

   (c) Sidelnikov bound [86]

$$R_{max}^2 \geq \begin{cases} \sqrt{2N}\ for\ binary\ sequences \\ \sqrt{N}\ for\ non-binary\ sequences \end{cases} \tag{2.6}$$

6. Linear span(L): If a sequence has a linear span of $L = p$, then by using $2p$ number of successive elements, the sequence can be predicted by using an algorithm such as continued fraction algorithm. Thus, the predictability and the cryptographic strength of a sequence is characterised by its linear span.

7. Pseudo-randomness: Sequences that satisfy the pseudo-random properties are known as pseudo-random sequences. The three properties of pseudo-randomness are [35]:

   (a) The out-of-phase periodic auto-correlation must be as small as possible. i.e.

   $$R_{i,i}(\tau) = \begin{cases} N, \tau = 0 \\ k, otherwise \end{cases} \tag{2.7}$$

   where k is a constant and its value must be as small as possible.

   (b) For every period, the number of 1s must be equal to the number of 0s.

   (c) For every period, half the period should be of single length, a quarter must be of length two, a eight, three and so on. A run here denotes consecutive string of identical alphabets.

2.1.2 Optimum Sequences

Selecting the family of optimum spreading sequences leads to maximising the network and information theoretic capacity[26, 81, 92]. It also optimises the transmit power and the receiver structure [26, 81, 92].

In [81] and [92] sequence sets that maximise the information theoretic capacity for a single cell synchronous single path DS-CDMA systems are investigated. Similarly [93] investigates sequence sets that maximises the network capacity. In both the cases it is shown that the information theoretic capacity and network capacity depends on the sequence sets used and by choosing optimal sequence sets the capacities can be maximised. For a given DS-CDMA system, if the number of users (K) is less than the processing gain (N), then orthogonal sequences like Walsh-Hadamard are optimal. While if the number of users is greater than the processing gain ($K > N$), then sequences satisfying the Welch bound on the total squared correlation with equality are optimal. Examples of such sequences are Gold sequences. They are also known as Welch bound equality (WBE) sequences

[91]. Gold sequences also satisfy the Sidelnikov bound with equality [35]. The orthogonal sequences namely Walsh-Hadamard sequences and WBE sequences namely Gold sequences are commonly known as optimal sets of sequences. These optimal sets of sequences are considered in this thesis.

2.2 Link Adaptation

Due to the broadcast nature, the wireless channel is shared by many users resulting in multiple access interference (MAI). To combat MAI, different strategies are adopted at both the transmitter and receiver. For example at the transmitter, power control and spreading sequence selection are adopted, while at the receiver, multi-user detection and receiver beam-forming strategies are adopted [26].

Optimal sequences do not have perfect zero cross-correlation property and hence are not perfectly orthogonal. This can cause degradation in system performance multiple access interference [91]. To counter this problem, power control is done to equalise received power per bit of all users. WCDMA uses fast closed loop power control by estimating the received signal-to-noise ratio (SIR) and comparing it with a target SIR [46].

Adaptive modulation and coding (AMC) is another method of link adaptation used in WCDMA that allows the power of the transmitted signal to be held constant over a frame interval. The modulation and coding format is adapted to match the channel condition of the user. Users closer to the base station experience better SIR and hence are allocated higher order resources of modulation and coding (64 QAM, 3/4 turbo codes) . While users away from the base station experience worse channel conditions and hence are allocated lower order resources of modulation and coding (QPSK, 1/3 turbo codes).

Optimum sequences are optimum with respect to their construction properties. Their usage allows to maximise network capacity, by reducing the interference. So the best one can do in terms of construction are optimum sequences. However, these sequences are allocated to users in a DS-CDMA system irrespective of the

users' channel condition. By allocating sequences to users based on their channel condition, the received power at the user can be maintained constant to maintain any give QoS. The method of choosing sequences based on users' channel condition is investigated in the thesis. In the next chapter, the principle concept of allocating sequences to users is presented with the help of different modeling methods namely simulation, analytical, and hardware model. Their performance is evaluated by gain achieved per link, complexity of computation and its overall effect on the system throughput.

2.3 Summary

Sequences denote variations of a pre-determined set of alphabets. Based on the type of alphabets they are broadly classified as binary and non-binary sequences. The characterisation of sequences involves properties such as; periodic and aperiodic correlation, linear span, and bounds namely; Welch bound, Sarawate bound, and Sidelnikov bound.

In general sequences with a large family size and decreased R_{max} are preferred. A sequence with large family size offers increased number of sequences for deployment. While a decreased R_{max} results in anti-fading characteristics of the sequences and also reduces cross-talk and interference among the users. However as the family size increases the value of R_{max} also increases. Due to the Welch bound it is also not possible to have sequences with both good auto and cross correlation properties. Thus a tradeoff is considered and sequences with specific properties of correlation and linear span are used in different applications like; direct sequence spread spectrum, RADAR, receiver synchronisation, GPS, and cryptography.

In terms of sequence design, optimum sequences are preferred for deployment in DS-CDMA systems as they maximise system performance. However increased system performance can be obtained by allocating the optimum sequences to users based on their channel condition. Similar to existing link adaptation techniques

such as power control and AMC, by allocating sequences to users based on their channel condition, the user can maintain a minimum received power to satisfy any given QoS. This method of channel aware adaptation is presented in Chapter 3 including various methods of validation and performance evaluation.

Chapter 3

Channel Aware Adaptation of Spreading Sequences

Spreading sequences are assigned to users to separate different links; uplink or downlink, in DS-CDMA. Generally sequences with good properties of periodic correlation are used for assignment such as the optimum sequences. Optimum sequences satisfy the orthogonal property or the Welch bound on total squared correlation with equality to maximise the information theoretic capacity of a single cell DS-CDMA system. Walsh-Hadamard sequences (when $K \leq N$, for K number of users and N spreading factor) and Gold sequences ($K > N$) are examples of optimum sequences. Generally, these sequences are assigned to users irrespective of their channel condition. In Chapter 3, we consider allocation of optimum sequences to users based on their channel condition in order to improve the performance of a DS-CDMA system.

In Section 3.2 using the link and system model, the principle concept of dynamically allocating sequences is discussed based on [84]. In Section 3.3 an optimum allocation scheme based on the Hungarian algorithm is proposed. Simulation results based on a downlink are derived. In Section 3.4 a fast but sub-optimum solution is proposed based on an analytical model. In Section 3.5 using real world channel measurements, the method is validated and its performance is also evalu-

ated. Finally the chapter is summarised in Section 3.6.

3.1 Principle of Dynamic Allocation of Sequences

3.1.1 The Link Model

A typical link model used in DS-CDMA consists of a transmitter, a channel, and a receiver as shown in Fig. 3.1. Without loss of generality and in order to keep the terminology simple, the transmission of only one symbol d is considered. At the transmitter, the digital information signal d of duration T is spread using a binary spreading sequence s of length N where $s = (s(0), s(1), \ldots, s(N-1))$ and $s(n) \in \pm 1$. Exactly one spreading sequence period of N chips per symbol duration T is assumed. The spread signal $d \cdot s(t)$ is transmitted over the multipath radio channel. The channel is described by its instantaneous channel impulse response $h = (h(0), h(1), \ldots, h(L-1))$ of L taps. Due to multipath propagation the transmitted signal undergoes multipath fading [90] and the received signal $e(t)$ is given by:

$$e(t) = d \cdot s(t) * h(t)$$

where $*$ denotes convolution.

At the receiver, a channel estimation unit is used to estimate h. The channel estimation information is now used by a sequence selection unit to select the "optimum" spreading sequence and inform the transmitter and the receiver on the selection. The sequence selection unit can either be implemented in the transmitter or the receiver. When implemented in the transmitter either a blind detection scheme for the used spreading sequence is required or the receiver needs to be informed about the selected spreading sequence; when implemented in the receiver, the transmitter needs to be informed about the chosen spreading sequence. In the latter case, additional signaling is required since the channel estimation information needs to be sent to the transmitter. Although the granularity of this signaling

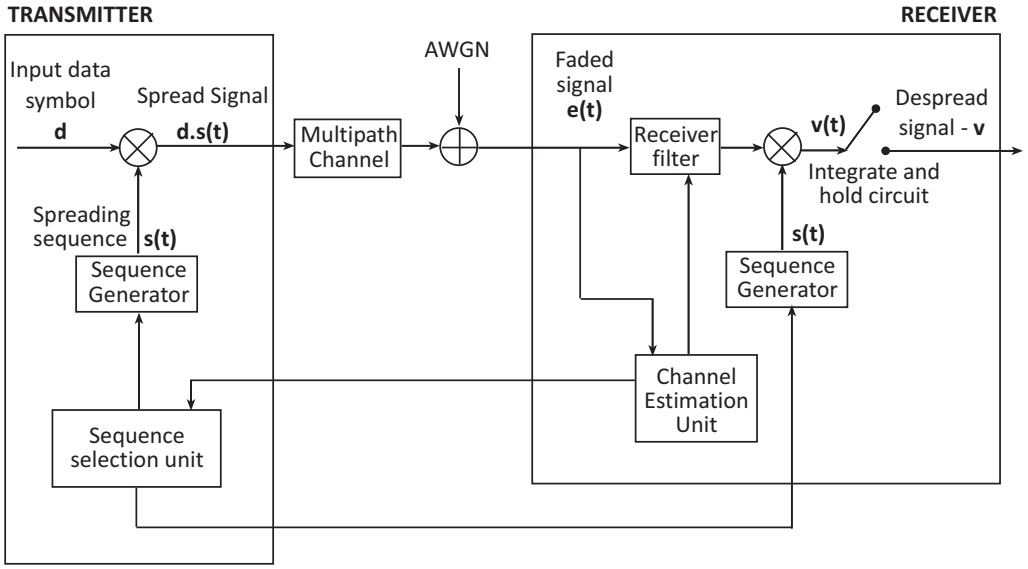

Figure 3.1: The Transmitter-Channel-Receiver Link Model

can be reduced, it will still require a higher bandwidth than just the information about the selected spreading sequence.

At the receiver, the incoming signal $e(t)$ will undergo a matched filtering for the fading channel (receiver filter) and will then be correlated with the spreading sequence, i.e., chip-wise multiplied by s and integrated (integrate and hold circuit). The latter step is the associated despreading operation for the spreading operation at the transmitter.

Assuming that only symbol d was sent, the signal at the output of the receiver sampled at $t = 0$ can be expressed by

$$v(0) = d \cdot s(t) * h(t) * h^*(-t) * s^*(-t)\|_{t=0} \tag{3.1}$$

3.1.2 The System Model

Spreading sequences are characterised by properties of correlation, periodicity, family size, maximum-linear span, and maximum non-trivial correlation. Cor-

relation is a measure of similarity between two sets of sequences and periodic correlation is pre-dominantly used to assert the worthiness of a sequence [35].

The need to consider aperiodic correlation of spreading sequences was first demonstrated by Anderson and Wintz [11]. In their paper Anderson and Wintz derived a bound on the signal-to-noise ratio at the output of a correlation receiver for a spread spectrum multiple access system with a hard limiter.

Considering equation (3.1) again:

$$v(0) = d \cdot s(t) * h(t) * h^*(-t) * s^*(-t)\|_{t=0}$$

It can be re-written as:

$$v(0) = d \cdot \tilde{C}_{ss}(t) * \tilde{C}_{hh}(t)\|_{t=0}$$

where
$\tilde{C}_{ss}(t)$ is the continuous-time aperiodic auto-correlation of the spreading sequence
$\tilde{C}_{hh}(t)$ is the continuous-time aperiodic auto-correlation of the impulse response of the channel.

The performance of a transmission scheme for BPSK and QPSK detection depends on the real part of the despread signal. Hence taking the real part of the despread signal from [84] we get:

$$\Re(v(0)) \sim v = d \cdot \Re(\sum_{m=0}^{N-1} C_{ss}(m) \cdot C^*_{hh}(m)) \tag{3.2}$$

where
$C_{ss}(m)$ is the discrete-time aperiodic autocorrelation of the spreading sequence,
$C_{hh}(m)$ is the discrete-time aperiodic autocorrelation of the impulse response of the channel.

The discrete-time aperiodic autocorrelation of a sequence with the period N is given by [35]

$$C_{aa}(\tau) = \sum_{n=0}^{N-1-\tau} a(n)a^*(n+\tau)$$

where $0 < \tau < N-1$. Since $C_{ss}(0) = N$, it is independent of the used spreading sequence, hence:

$$v = d \cdot NC^*_{hh}(0) + d \cdot \Re(\sum_{m=1}^{N-1} C_{ss}(m) \cdot C^*_{hh}(m)) \tag{3.3}$$

The first term in the above equation consists of constants N and d and hence is invariant. In the second term, $C_{ss}(m)$ is determined by the spreading sequence $s(t)$ while $C_{hh}(m)$ is determined by the state of the channel $h(t)$ at a time t. $C_{hh}(m)$ cannot be varied since it depends on the channel condition $h(t)$, but $C_{ss}(m)$ can be varied depending on the spreading sequence $s(t)$.

$$\sum_{m=1}^{N-1} C_{ss}(m) \cdot C^*_{hh}(m) \tag{3.4}$$

So, we can choose a spreading sequence $s(t)$ with the discrete-time aperiodic autocorrelation $C_{ss}(m)$ such that (3.4) is maximised. Maximising (3.4) increases the magnitude of the value of despread signal v, and the power of the received signal. Thus the main principle of allocating spreading sequences based on channel conditions is to chose a sequence $s(t)$ such that for a given channel condition $h(t)$, the magnitude of (3.3) is maximised.

3.2 Simulation Model

High-Speed Downlink Packet-Access(HSDPA) is the first evolution step towards Third Generation (3G) mobile technology. The key idea behind HSDPA is to improve the packet data throughput using existing GSM and EDGE standards [46]. A simplified down-link model of HSDPA is shown in Fig. 3.2. It consists of a base station serving 15 users, here called User Equipments (UEs). The transmission between the base station and a user is described by the above defined down-link model. The 15 UEs are assumed to have mutually independent channel impulse responses.

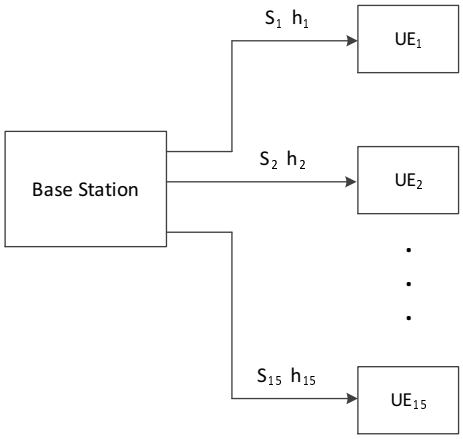

Figure 3.2: Basic HSDPA Model

3.2.1 Optimum Allocation

In order to allocate the sequences S_i based on the channel conditions h_j, equation (3.3) can be re-written as:

$$V_{i,j} = d \cdot NC^*_{hh}(0) + d \cdot \Re(\sum_{m=1}^{N-1} C_{ssi}(m)C^*_{hhj}(m)) \tag{3.5}$$

where $i = j = 1, 2, \ldots, 15$.
$C_{ssi}(m)$ is the discrete time aperiodic autocorrelation of the spreading code S_i
$C_{hhj}(m)$ is the discrete time aperiodic autocorrelation of the channel condition h_j.
Thus,

$$V_{i,j} = \begin{bmatrix} V_{1,1} & V_{1,2} & V_{1,3} & \ldots & V_{1,14} & V_{1,15} \\ V_{2,1} & V_{2,2} & V_{2,3} & \ldots & V_{2,14} & V_{2,15} \\ V_{3,1} & V_{3,2} & V_{3,3} & \ldots & V_{3,14} & V_{3,15} \\ . & . & . & \ldots & . & . \\ . & . & . & \ldots & . & . \\ . & . & . & \ldots & . & . \\ V_{15,1} & V_{15,2} & V_{15,3} & \ldots & V_{15,14} & V_{15,15} \end{bmatrix}$$

Now the idea is to choose and allocate spreading sequences with the value of de-spread signal $V_{i,j}$ from the above matrix such that the overall system performance is maximised [8, 9]. To chose sequence $S_i(t)$ for channel condition $h_j(t)$ such that the assignment of codes to users is maximum over all the other assignment.

$$Maximize \sum_{i,j} V_{i,j} h_{i,j} \tag{3.6}$$

for a given cost

$$C = max\ V_{i,j}$$

$$Minimize \sum_{i,j} \{C - V_{i,j}\} h_{i,j}$$

$$Minimize \sum_{i,j} -V_{i,j} h_{i,j}$$

subject to constraints

$$\sum_{j} h_{i,j} = 1$$

$$\sum_{i} h_{i,j} = 1$$

This allocation problem is known as an assignment problem in the operations research literature [79]. The assignment problem deals with the allocation of an exclusive resource, from the source node to the destination node such that the overall cost is maximised (or minimised, depending on the cost parameter). The Hungarian algorithm provides an optimum solution for the assignment problem [79].

Hence by using the Hungarian algorithm, spreading sequences can be chosen from the matrix $V_{i,j}$ and allocated optimally to each UE. For the case $K = 15$ users Walsh-Hadamard sequences are allocated while, for the case $K = 33$ users Gold sequences of period $N = 31$ are allocated.

3.2.2 Performance Evaluation of Simulation Model

Monte-Carlo Simulations

To evaluate the performance of the simulation model, the achievable gain and the computational complexity of the Hungarian allocation scheme, is calculated based on the down-link physical layer as shown in Fig. 3.3. The modules of the transmitter-channel-receiver are built in IT++[89]. For each channel realisation, 50,000 Monte-Carlo simulations are performed. The channel realisations include; Indoor channel (1-tap), ITU Pedestrian A(4-tap), ITU Vehicular A(6-tap) channel models.

Achievable Gain

Let SNR_{dyn} be the the signal-to-noise ratio(SNR) of the the downlink, that allocates sequences dynamically to users based on their channel condition, while SNR_{stat} be the SNR of the downlink that allocates sequences statically to users irrespective of their channel condition. Then the gain achieved is:

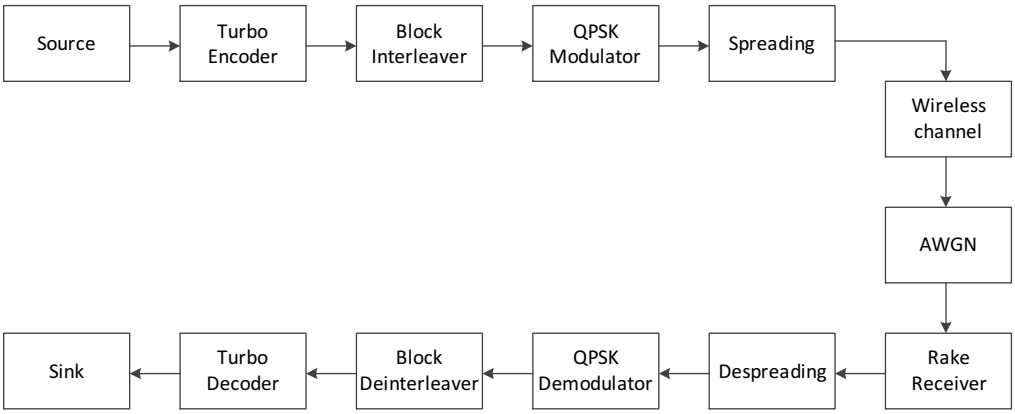

Figure 3.3: Functional Block Diagram of Downlink Physical Layer.

$$Gain = \frac{SNR_{dyn}}{SNR_{stat}} \tag{3.7}$$

where

$$SNR = \frac{v^2}{N_0 + I} \tag{3.8}$$

where v is the energy of the received signal and $N_0 + I$ is the multi-path interference.

The gain achieved for each set of sequences namely; Walsh-Hadamard sequences and Gold sequences is shown in Table 3.1

Table 3.1: Gain(dB) Achieved from Monte-Carlo Simulations .

Gain in dB	Walsh-Hadamard sequences (K=15) users	Gold sequences (K = 33)users
ITU PA(4 tap)	2.89 dB	1.15 dB
ITU VA(6 tap)	1.17 dB	1.07 dB

Downlink Load Factor

To calculate the theoretical spectral efficiency of a cell in HSPA using dynamic allocation of sequences, the downlink load factor η_{DL} is calculated as illustrated in [46] Eqn. 3.9.

$$\eta_{DL} = \sum_{j=1}^{N} v_j \cdot \frac{(E_b/N_o)_j}{W/R_j} \cdot [(1 - \alpha_j) + i_j] \tag{3.9}$$

where,

- N: number of users per cell,
- v_j: activity factor of user j at physical layer, 0.58 for speech,
- E_b/N_o: Signal energy per bit to noise spectral density,
- W: WCDMA chip rate, 3.84 Mcps,
- R_j: Bit rate of user j, 16 kbps for adaptive multi-bit rate wideband codec,
- α_j: Orthogonality of channel user j, 1 for fully orthogonal channel,
- i_j: Ratio of other cell to own cell base station power, Macro-cell with omni-directional channel 55 %.

A comparison of the system throughput for Walsh-Hadamard sequences obtained for different spreading factors namely; 16, 32, 64, and 128 are as shown in Fig. 3.4.

A comparison of the system throughput for Gold sequences obtained for different spreading factors namely; 31, 63, and 127 are as shown in Fig. 3.5.

Expected Value

The expected value of gain (in dB) is also calculated by using the following equation

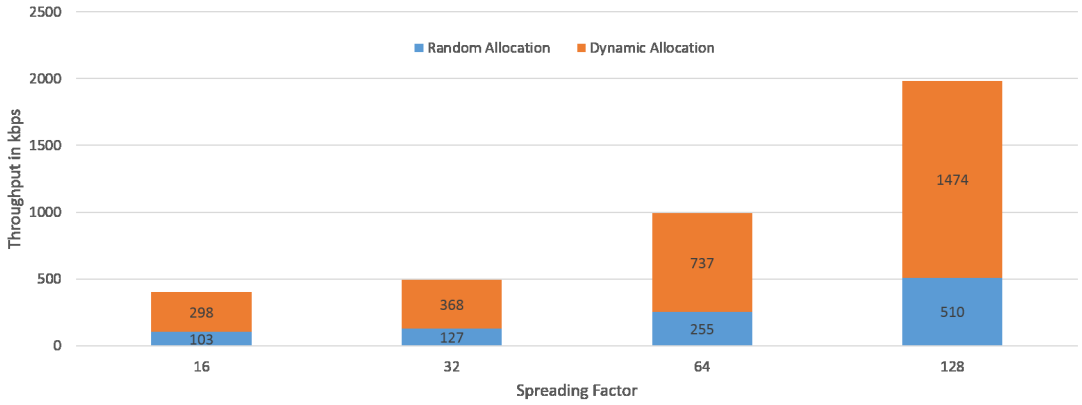

Figure 3.4: Throughput comparison for Walsh-Hadamard sequences.

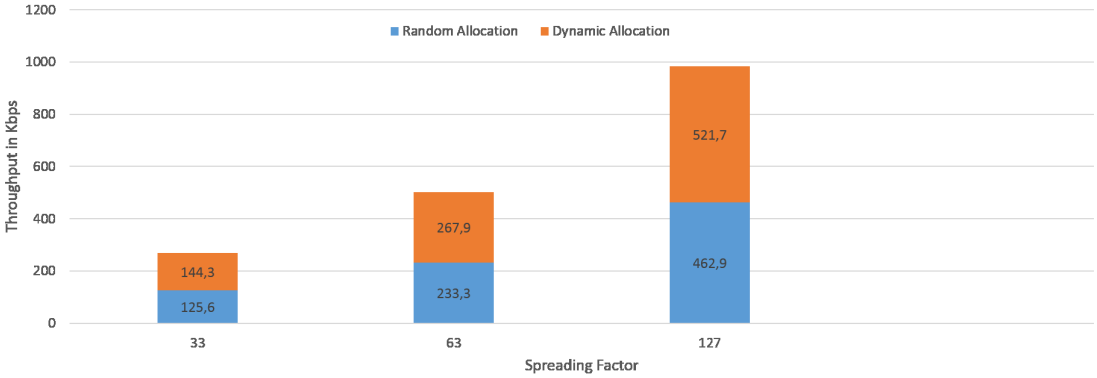

Figure 3.5: Throughput comparison for Gold sequences.

$$E[gain] = \frac{E[SNR_{dyn}]}{E[SNR_{stat}]} \tag{3.10}$$

where $E[\,]$ is the value of expectation.

$$E[gain] = \frac{E[v_{dyn}^2]}{E[v_{stat}^2]}$$

$$E[gain] = \frac{E[d \cdot NC_{hh}^*(0) + d \cdot \Re(\sum_{m>0} C_{ss}(m)C_{hh}^*(m))]^2}{E[d \cdot NC_{hh}^*(0) + d \cdot \Re(\sum_{m>0} C_{rr}(m)C_{hh}^*(m))]^2} \tag{3.11}$$

where $C_{ss}(m)$ is the aperiodic autocorrelation of the dynamically allocated spreading sequence $s(t)$, $C_{rr}(m)$ is the aperiodic autocorrelation of the statically allocated spreading sequence $r(t)$, and $C_{hh}(m)$ is the aperiodic autocorrelation of the channel condition $h(t)$. Since $s(t)$ is chosen based on the channel condition $h(t)$ equation (3.11) can be simplified as:

$$E[gain] = \frac{[d \cdot NE[C_{hh}^*(0)] + d \cdot \Re(\sum_{m>0} E[C_{ss}(m)C_{hh}^*(m)])]^2}{[d \cdot NE[C_{hh}^*(0)] + d \cdot \Re(\sum_{m>0} E[C_{rr}(m)]E[C_{hh}^*(m)])]^2} \tag{3.12}$$

The expected value of the gain for both Walsh-Hadamard sequences and Gold sequences for different channel realisations is as shown Table 3.2.

Table 3.2: Expected Value of Gain.

Gain in dB	Walsh-Hadamard sequences (K=15) users	Gold sequences (K = 33)users
ITU PA(4 tap)	4.57 dB	3.50 dB
ITU VA(6 tap)	3.19 dB	2.78 dB

Effect of Inter-symbol-interference

As seen in Tables 3.1 and 3.2, the expected value of the gain is higher than the gain obtained from the simulation model. In the IT++ based simulations, due to smearing of the symbols, a reduction in the SNR of the received signal is observed. As the effect of ISI is not seen during the expected value calculations hence the gain obtained using expected value is greater than gain obtained during the IT++ simulation model.

Computational Complexity

To compute the computational complexity of the Hungarian allocation scheme, the Big O notation is considered. Equation (3.3) consists of N additions and N multiplications. Hence the complexity of (3.3) is $O(N)$. Using (3.5) the matrix $V_{i,j}$ is calculated that consists of K^2 elements, where K is the number of users in the down-link. Hence the complexity to construct the matrix is $O(K^2)$. The computational complexity of choosing K optimum elements from K^2 elements is $O(K^3)$ [79]. Thus the overall computational complexity of the Hungarian allocation scheme is $O(K^3 + K^2 + N) = O(K^3)$.

3.3 Fast, Sub-optimum Allocation

The Hungarian based dynamic allocation scheme is an optimal solution for allocating sequences. However the tradeoff in obtaining the gain is a high degree of computational complexity i.e. $O(K^3)$. Hence the motivation for an analytical model is, to devise a scheme that can allocate sequences with reduced computational complexity, and yet can achieve similar performance as compared to the Hungarian scheme. The results of Monte-Carlo simulations obtained in the simulation model is visualised to obtain clusters of sequences and channel conditions as shown in Fig. 3.6.

The visualisation indicates a mapping of the channel conditions and its cor-

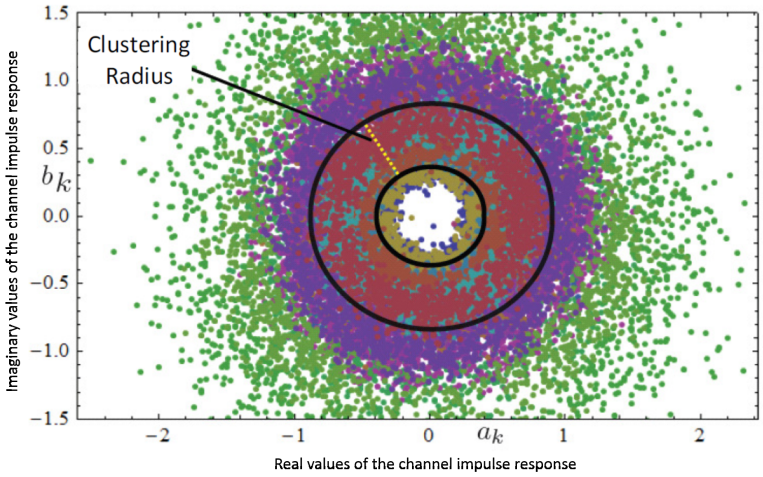

Figure 3.6: Cluster Visualisation of Monte-Carlo Simulations.

responding allocated sequence. Based on this visualisation, the 15 concentric regions are identified that correspond to the 15 allocated Walsh-Hadamard sequences. By applying a convex hull on to the 15 concentric regions, 15 concentric circles of radii r_i are obtained as shown in Fig. 3.7. Each circle represents a region within which if a channel condition is mapped, then that sequence (circle) can be allocated to it. Now to allocate sequences to users, the radii r_i of concentric circles is calculated. Each radius represents a sequence. Hence the order of the sequence from the inner most to the outer most circle is calculated.

To allocate sequences to K users, the users' channel conditions are mapped on to the concentric circles. For each user, the distance w.r.t. the origin is calculated and arranged in the ascending order. Let $\hat{S}$ be the order of the sequence obtained from the concentric circles. Then the inner most circle would be $\hat{S}_1$ and outer most circle be $\hat{S_{15}}$. The user nearest to the inner circle is allocated the code $\hat{S}_1$ while the user nearest to the outermost code is allocated the code $\hat{S_{15}}$. Thus a pseudo-dynamic allocation of sequences to users based on their channel condition is achieved [21]. This procedure is also repeated for Gold sequences to obtain similar concentric regions and circles. In this case since 33 users are considered,

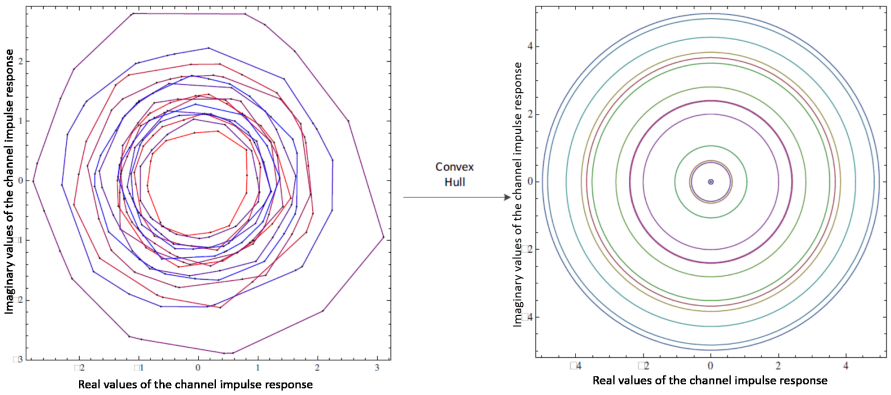

Figure 3.7: Mapping clusters into concentric circles through convex hull.

33 concentric circles are obtained. The users are similarly mapped onto the circles and accordingly allocated.

The Monte-Carlo visualisation yields the pattern of channel condition-to-sequence allocated cluster. By using this pattern the pseudo-dynamic allocation of sequences is achieved. The calculation of the distances of the users w.r.t. the origin of concentric circles is the only computation that needs to be done thereby reducing the cost of allocation.

3.3.1 Performance Evaluation

The gain achieved by pseudo-dynamically allocating sequences to users for Walsh-Hadamard sequences of SF=16 is upto 1.80 dB per link for ITU pedestrian A channel(4tap). While for Gold sequences with SF=31 the gain obtained is upto 0.94 dB per link.

The order of the sequences obtained from the concentric circles is derived through the Monte-Carlo simulations. Once the order is established by computing the shortest distance, a pseudo-dynamic allocation of sequences can be achieved. Hence the complexity is based on complexity of calculating the distance of the channel condition w.r.t. the origin. Hence the complexity of calculating the dis-

tance is $O(1)$.

3.4 Hardware Model

Introduction to Software Defined Radio(SDR)

Traditionally hardware validation of transceiver modules has been through either custom built RF circuits or through Application Specific Integrated Circuits(ASICs). The process usually consists of building functional block-sets of the transceiver modules in Hardware Description Language(HDL) like VHDL or Verilog. Then a net-list is derived from the HDL modules that can be mapped on to Field Programmable Gate Arrays(FPGA). The mapped net-list is validated by using custom built FPGA kits with suitable RF front-ends.

However this approach needs expertise in modeling HDL modules, mapping and validating it on, FPGA kits. A recent trend has been to validate transceiver modules on Software Defined Radio(SDR). Software defined radio is an evolution of custom defined radio frequency(RF) circuits. The term software defined radio means that the radio functionalities are defined in a software like MATLAB, SIMULINK, GNURADIO, GNU Radio, Companion(GRC) and they can be implemented on a general purpose hardware with RF-frontends, instead of custom designed RF circuits [69, 3, 18]. The hardware platform is capable of receiving data from any frequency band (or at least some of the frequency bands) and can demodulate the received signal in a software defined baseband.

The advantage of SDR is that the transceiver modules are defined in software and then validated through the RF interface using real world channel measurements. Any change or improvement to the transceiver modules can be easily done through the software while they can still be validated using real world channel measurements. And since one of the main objectives of the thesis is to validate the key generation algorithms using real world channel measurements, the SDR is a preferable testbed platform.

Currently many commercial SDR hardware platforms are available such as;

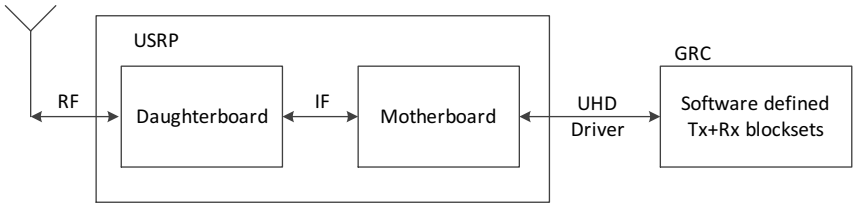

Figure 3.8: Functional Block Diagram of USRP.

the Universal Software Radio Peripheral(USRP), SOftware developed RAdio(SORA), and Lyrtech. There are also many software platforms available for building the functionalities of the transceiver modules such as; MATLAB, SIMULINK, GNU Radio[80], and GNU Radio Companion(GRC)[25]. The GNU Radio environment provides an open source platform to develop transceiver modules in C++. The control and data flow between the modules are defined in Python scripts. GRC is a GNU Radio based graphical user interface(GUI) programming tool that consists of pre-defined transceiver modules.

The SDR platform considered for this thesis is the USRP and the open-source GRC tool is used to define the software defined baseband transceiver modules. The functional block diagram of USRP and GRC is as shown in Fig. 3.8.

Working Model of USRP

The USRP has three important building blocks namely; the software defined blocks sets, the motherboard, and the daughter board. The software defined baseband processing block-sets are defined in GRC. Through a UHD driver, the baseband modules are then mapped onto the FPGA while transmitting or receiving the data in real-time. On the motherboard, the baseband digital signal is converted to a baseband analog signal through the Digital-to-Analog converter (DAC). The analog signal is then up-converted to a specified radio-frequency(RF) for transmission through the daughter boards. The associated steps from the software defined block sets to the RF transmission, involves transmitting the data. The reception of

data consists of receiving the data from the RF front-end, down-converting it to an intermediate frequency, analog to digital conversion and to subsequently processing it on the software defined modules. The specifications of the USRP used are indicated in Table 3.3.

Table 3.3: Specifications of the Software Defined Radio.

Software	GNU Radio Companion
Motherboard	USRP N210
FPGA	Xilinx Spartan 3A-DSP 3400 FPGA
ADC	100 MS/s dual ADC
DAC	400 MS/s dual DAC
Connectivity	Gigabit Ethernet
Daughter board	WBX (50-2200 MHz)
Antenna	3dBi gain Vert900

USRP-GRC Setup

The functional block diagram of the transmitter and receiver is as shown in Fig. 3.9. The transmitter module consists of a linear feedback shift register(LFSR) as the source. It produces a maximal-length pilot sequence(m-sequence) [35] in bipolar alphabets $\{1, -1\}$. The bits are then amplified and transmitted through the USRP. Each packet transmitted is of 63 bits length. The data transmission happens in the ISM band (ZigBee network [15]) at a frequency of 864 MHz.

As already discussed in Chapter 2, m-sequences have good periodic autocorrelation property, i.e. they have a peak at the zero-delay and a very small value at the out-of-phase correlation values. As a result of this property synchronisation of each block of received data is relatively easier. By correlating the received signal to a corresponding m-sequence of the same length and order, as shown in Fig. 3.9, the peaks at the beginning of every data block is calculated. This information

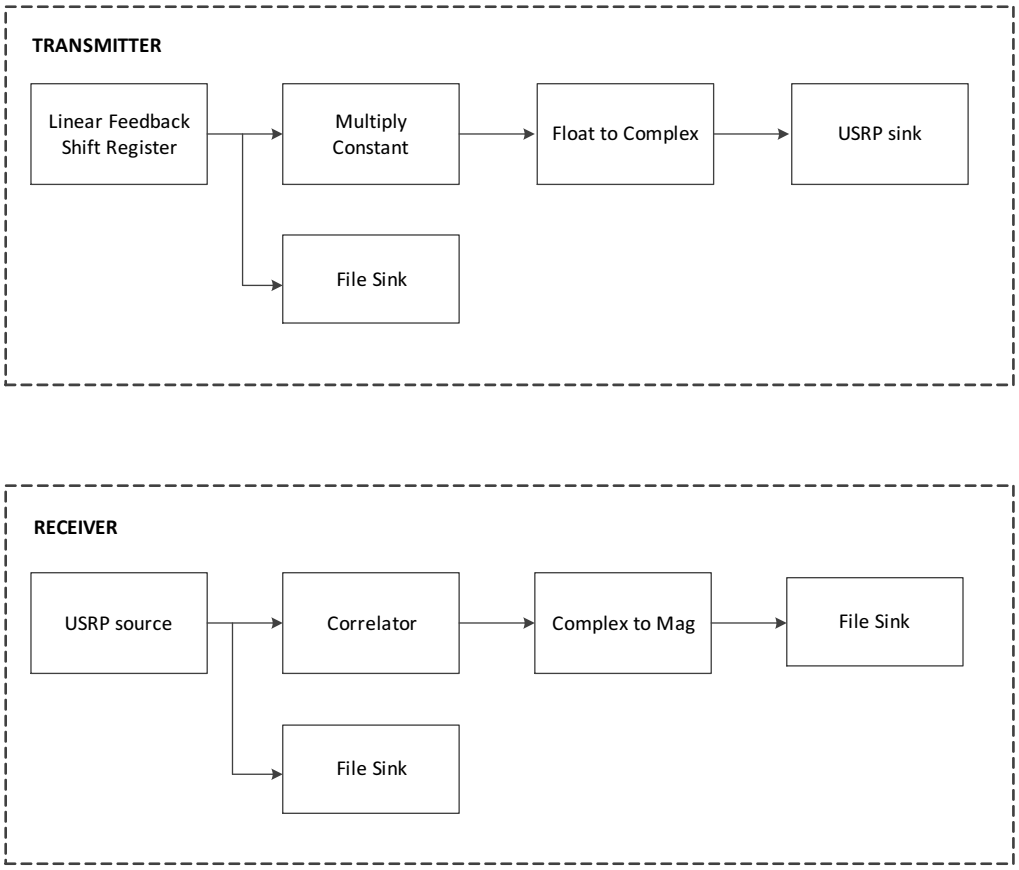

Figure 3.9: Functional Block Diagram of Transmitter and Receiver.

is utilised to synchronise the received data. Once the blocks of data and their timing information are recovered, the impulse response of the channel is estimated by; a) calculating the number of taps b) co-efficient of the impulse response of the channel.

Least Square Channel Estimation

The received signal is autocorrelated with itself to identify multiple peaks in the autocorrelated signal. The multiple peaks signify the number of times the same data block has been received due to the multi-path transmission through the wire-

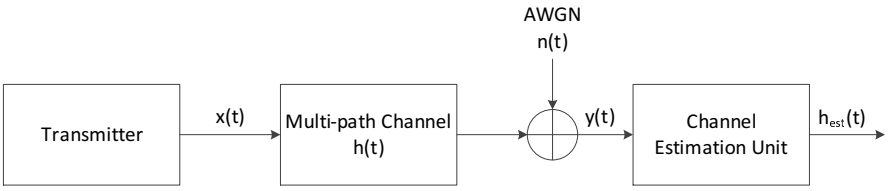

Figure 3.10: Least Square Channel Estimation.

less channel. Thus by thresholding the peaks, the number of taps of the impulse response of the channel is calculated. Once the number of taps are calculated, the value of co-efficient i.e. the amplitude and phase of the impulse response is calculated using the Least Square Estimation method [77, 54].

To estimate the impulse response of the channel, let us assume a signal source that transmits a training sequence $x(t)$ at the transmitter as shown in Fig. 3.10. The received signal $y(t)$ can be expressed as:

$$y(t) = x(t) * h(t) + n(t) \tag{3.13}$$

where, $*$ is the convolution operator, $h(t)$ is the impulse response of the channel and $n(t)$ is the Additive White Gaussian noise(AWGN).

Re-writing it in the matrix form:

$$y = Xh + n \tag{3.14}$$

where $h = [h_0, h_1, \ldots h_L]^T$ is the L tap impulse response of the channel.

$x = [x_0, x_1, \ldots, x_{P+L-1}]^T$ is the training sequence with the reference length P.

The circulant training sequence matrix X is then given by

$$X = \begin{bmatrix} x_L & \dots & x_1 & x_0 \\ x_{L+1} & \dots & x_2 & x_1 \\ . & \dots & . & . \\ . & \dots & . & . \\ . & \dots & . & . \\ x_{L+P-1} & \dots & x_P & x_{P-1} \end{bmatrix}$$

Assuming AWGN noise, the best linear unbiased least square estimate of the impulse response of the channel is given by [77, 54]:

$$h_{est} = (X^H X)^{-1} X^H y \tag{3.15}$$

where X^H is the Hermitian and X^{-1} is the inverse of the matrix X.

For a training sequence with an ideal periodic autocorrelation, (3.15) can be simplified as [77, 54]:

$$h_{est} = \frac{1}{P} X^H y \tag{3.16}$$

3.4.1 Proof-of-Concept

Experiment Methodology

The experimental setup used to obtain real world channel estimates is as shown in Fig. 3.11. It consists of two USRPs, one as the transmitter and the other as the receiver configured in a simplex mode. The experiment is conducted in indoor lab and outdoor university campus. The indoor measurements yield single-tap channel measurements. While the outdoor channel measurements yield channel estimates from one-tap to four-taps. Based on these channel estimates, spreading sequences are allocated to users of a down-link model as shown in Fig. 3.3.

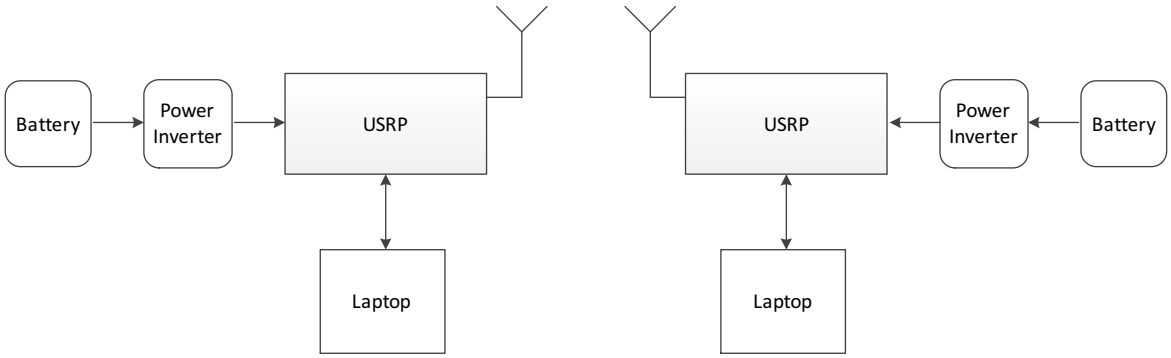

Figure 3.11: Outdoor USRP Setup.

3.4.2 Performance Evaluation of Hardware Model

Based on equation 3.7, the gain is calculated for each realisation. The gain achieved for each set of sequences namely; Walsh-Hadamard sequences and Gold sequences is shown in Table 3.4.

Table 3.4: Gain Achieved from Hardware Model.

Gain in dB	Walsh-Hadamard	Gold
Outdoor (2 tap)	0.21 dB	0.34 dB
Outdoor (3 tap)	0.84 dB	0.68 dB
Outdoor (4 tap)	0.92 dB	0.85 dB

3.5 Summary

Spreading sequences are usually characterised by the properties of periodic and aperiodic correlation. They are usually allocated to users irrespective of their channel conditions. In this chapter the principle concept for allocating sequences to users based on their channel condition was discussed.

For a given channel condition $h(t)$, a sequence $s(t)$ is chosen such that the product of their aperiodic autocorrelation is maximised. By maximising their product, the magnitude of the energy of the received signal is maximised. Thus spreading sequences can be allocated to users based on their channel condition.

By considering a simplified downlink model, the sequences are allocated to users dynamically based on their channel condition. The dynamic allocation is based on an optimal allocation scheme known as the Hungarian algorithm. A performance gain of up to 2 dB per user is achieved in the downlink, consisting of $K = 15$ users for Walsh-Hadamard sequences. Whereas in case og Gold sequences, a gain of up to 1 dB per user is achieved. The computational complexity of allocation scheme is $O(K^3)$.

The optimal Hungarian algorithm is computationally intensive. To combat this problem a sub-optimal but fast allocation scheme is proposed through an analytical model. The analytical model consists of a step function that allocates pseudo-dynamically instead of dynamically. A similar performance is obtained with a gain of up to 2 dB for Walsh-Hadamard sequences and a gain of up to 1 dB for gold sequences at a reduced computational complexity of $O(1)$.

As a proof-of-concept, real world channel estimates are obtained by using a software defined radio platform USRP.

Thus, by evaluating different methodologies namely simulation model, analytical model, and a proof-of-concept based on a hardware model, spreading sequences are allocated to users based on their channel condition.

Chapter 4

Physical Layer Security: State of the Art

4.1 Introduction

In tune with Moore's law[70], a rapid increase in computing and communication power, and a significant decrease in the size and cost of hardware, has lead to a increased deployment of mobile and vehicular ad-hoc networks. Such deployments can be broadly classified under the umbrella of Cyber Physical Systems [34]. Examples of such deployments include;

1. Ambient assisted living [87, 101] that provide on-time assistance to elder people and thereby aide them in living a better life.
2. Car to Car communication[27, 39, 60] that enhances the convenience of drivers by giving them real-time information about, traffic conditions, weather, accident spots, and entertainment services. This could greatly improve the safety and reliability of road transport.
3. Deployment of cyber physical systems in the industry to help improve production efficiency, communication between devices, and configurability of devices.

Hence machine to machine (M2M) communication will grow rapidly, improving communication and enhancing system capabilities. However this will also increase the heterogeneity of the systems and their ability to access information from various points of source. Given the mobility and broadcast nature of the channel, security will be an important and necessary condition for wireless ad-hoc networks. Since it is only security that will entitle the ad-hoc networks to function, seamlessly and effectively. It is these aspects of security that are introduced in this chapter.

The organisation of this chapter is as follows; in Section 4.2 a broad overview of security in wireless ad-hoc networks is presented. In Section 4.3 the main principle of channel reciprocity is discussed. The state of the art of physical layer security is presented in Section 4.4. Section 4.5 deals with the evaluation metrics used to validate the key generation algorithms of physical layer security. The need for better methods is reasoned in Section 4.6 and lastly the chapter is summarised in Section 4.7.

4.2 Security in Wireless Ad-hoc Networks

The attributes of security in an ad-hoc network are [105]; *availability*, *confidentiality*, *integrity*, *authentication*, and *non-repudiation* of the nodes.

1. *Availability*: Availability indicates that the network can survive any form of an attack by an adversary and yet be able to function normally. For instance an active adversary can launch denial of services attack on any layer of the network and effectively jam all services. Inspite of such an attack, the network must be able to function properly.

2. Confidentiality: All communication happening between the authorised nodes must not be accessible to the unauthorised nodes. Especially when ad-hoc networks are entrusted with sensitive information, confidentiality of the data must be maintained at all times.

3. Integrity: The integrity of the data transferred between nodes must remain incorrupt. All destined nodes must receive the data in an original and uncorrupted form.

4. Authentication: The authenticity of the network is determined by an unique identity of each node. By uniquely identifying each node, duplication and forgery can be avoided.

5. Non-repudiation: All communicating nodes must be held responsible for the data transmitted by them. This is to ensure the validity of the data from its originating node.

An ad-hoc network satisfying all of the above mentioned attributes is secure. If these attributes are not satisfied then, the network could be exposed to threats like *forgery*, *data deletion*, *modification*, *sniffing*, *denial-of-service attacks*, and *man-in-the-middle attacks*.

The confidentiality of the communication between nodes is ensured by encryption and decryption of messages. Encryption involves converting the original data into unreadable data using a cipher paired with, a secret key. While decryption is the reverse process of encryption. By using the same secret key and a decipher algorithm, the original data is recovered.

For effective encryption-decryption of information, it is necessary to have secret key management systems. The mobility and broadcast nature of wireless channel makes it important to have effective key management systems. Key management systems are usually centralised. A central *Certifying Authority* is responsible for managing keys among the nodes of the network. It makes sure that all nodes have the necessary secret keys and from time to time they are refurbished as necessary. Such a system is suitable for a fixed and non-scalable network. But in case of mobile and vehicular ad-hoc networks, the topology of the network keeps changing dynamically, hence it is not realistic to have a centralised authority. Moreover a compromise of the certifying authority could compromise the confidentiality of the whole network. Thus, it is desirable to have a distributed

system wherein each node is responsible for their own key management system.

Conventional secret key management systems employ computational cryptographic methods like, symmetric [13] and asymmetric key management systems. Symmetric key management systems are computationally less intensive but depend on a common shared channel. While asymmetric key generation methods are secure but are computationally intensive. Employing conventional key management methods has certain limitations such as;

1. Constraints in terms of computational power and energy limitations of the nodes limit the usage of asymmetric key generation schemes.

2. Due to bandwidth limitations, the exchange of high entropy keys is very expensive.

3. Most of the ad-hoc networks lack online connections to servers that serve Certificate Revocation Lists(CRL), thereby making it hard in implementing a conventional certificate based key management system.

Hence alternate methods of key management are necessary. One such alternate method that can adapt to the channel conditions and can be effectively deployed is *Physical Layer Security* [40, 44]. By using the reciprocal and random variations [50] of the wireless channel, a shared secret key can be established between a pair of nodes of an ad-hoc network. Recently such methods have been proposed and deployed in the state of the art such as in ;

1. Indoor wireless sensor networks(WSN)[98, 99, 100, 66, 67],

2. Ultra Wide Band(UWB) networks [64, 62],

3. Peer-Peer networks [88, 45, 78, 82, 47, 24]

4. Multiple Input Multiple Output(MIMO) systems [76, 94, 97, 103]

5. Orthogonal Frequency Division Multiplexing(OFDM) systems [55]

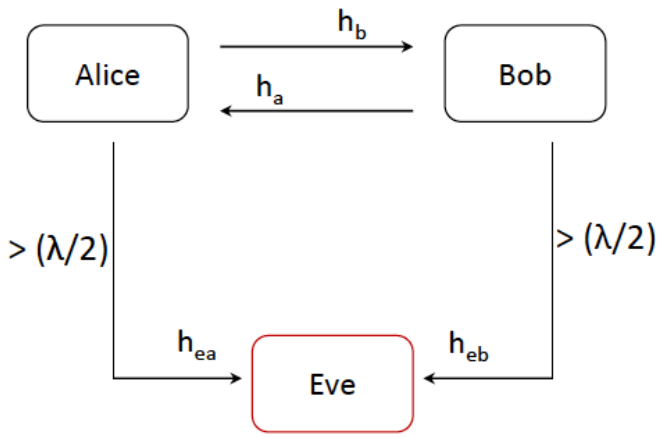

Figure 4.1: Need for secrecy.

6. Mobile radio [41, 57, 65, 12, 51, 36]

Physical layer security offers an unique solution to the problem of key management. By profitably exploiting the fading characteristics of the channel, key management systems can be deployed in a cost effective manner. Once such systems are integrated, the application layer based encryption-decryption algorithms, can extract the secret key from the physical layer. Without the need of any certifying authority, key management can be done in a modular and scalable manner. A survey on such methods of key generation schemes currently proposed in the state of the art is presented in the next section.

4.3 Principle of Channel Reciprocity

Fading is an inherent characteristic of the wireless channel due to which variations in the amplitude and phase of the transmitted signal occur. Let us consider two legitimate nodes of a wireless ad-hoc network named Alice and Bob as shown in Figure 4.1. Let Eve be an adversary node that is passively eavesdropping on all the communication between Alice and Bob. Let,

- $s(t)$ be a pilot sequence transmitted at time t

- $r_a(t)$ and $r_b(t)$ be the received signal at Alice and Bob respectively,

- $h_a(t)$ and $h_b(t)$ be the channel measurements of the multi-path channel measured by Alice, and Bob respectively,

- $n_a(t)$ and $n_b(t)$ be the additive white Gaussian noise experienced at Alice and Bob respectively.

Then the impulse responses, $h_a(t)$ and $h_b(t)$ can be expressed as shown in (4.1).

$$r_a(t) = s(t)h_a(t) + n_a(t) \tag{4.1}$$

$$r_b(t) = s(t)h_b(t) + n_b(t)$$

While let,

- $r_{ea}(t)$ and $r_{eb}(t)$ be the received signal at Eve due to Alice and Bob respectively

- $h_{ea}(t)$ and $h_{eb}(t)$ be the channel measurement measured by Eve due to Alice and Bob respectively ,

- $n_e(t)$ be the AWGN noise at Eve.

Then the impulse response measured at Eve can be expressed as shown in (4.2).

$$r_{ea}(t) = s(t)h_{ea}(t) + n_e(t) \tag{4.2}$$

$$r_{eb}(t) = s(t)h_{eb}(t) + n_e(t)$$

The principle of channel reciprocity [50] indicates that, the channel measurements ($h_a(t) \sim h_b(t)$) when they are measured during the coherence time of the channel. If λ is the wavelength of the wave transmitted between Alice and Bob, and if we assume that Eve is ($\lambda/2$) times away from both Alice and Bob then, ($h_{ea}(t) \neq h_a(t)$) and ($h_{eb}(t) \neq h_b(t)$). Even though Eve has access to the transmitted pilot sequence $s(t)$, the channel measurement measured by Eve w.r.t Alice and Bob will not be the same. For example if Alice and Bob communicate at 2.4 GHz frequency, and if Eve is more than $\lambda/2 = 6.25$ centimetres away from both Alice and Bob then equation (4.2) holds true. As seen in Figure 4.2, the principle of channel reciprocity can be verified. Alice and Bob communicate at 2.4 GHz frequency and conduct their channel measurements by measuring the received signal strength indicator(RSSI). Eve is placed at a distance greater than 6.25 centimeters from both Alice and Bob and in turn measures it's RSSI. As seen from the figure, Alice and Bob measure similar variations of RSSI while Eve does not measure similar RSSI variations. This is due to the principle of channel reciprocity. Hence by using such similar, reciprocal, and random channel variations, a shared secret key can be established between Alice and Bob. Thus an inherently harmful characteristic of the wireless channel such as multi-path fading, can be exploited profitably to build effective secret key management systems between a pair of nodes in an ad-hoc wireless network.

4.4 Standard Method of Key Generation

The standard procedure of extracting secret keys consists of four important steps as shown in Figure 4.3 namely:

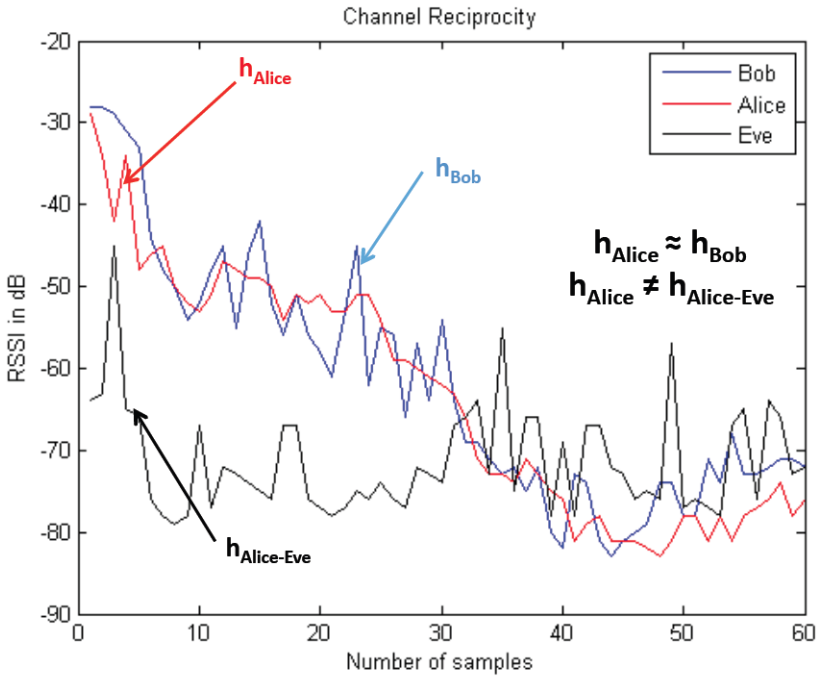

Figure 4.2: Principle of Channel Reciprocity.

1. Channel measurement
2. Quantisation
3. Information reconciliation
4. Privacy amplification

As a first step, the channel is probed at both the nodes to measure the variations of the channel within the coherence time, to obtain a *channel profile*. The channel profile is then quantised to obtain a *preliminary key*. Due to variations in the channel profile, the preliminary key constructed at both the ends do not match for all the bits. Hence to synchronise the preliminary keys, error detection and correction methods are used during the information reconciliation stage to obtain

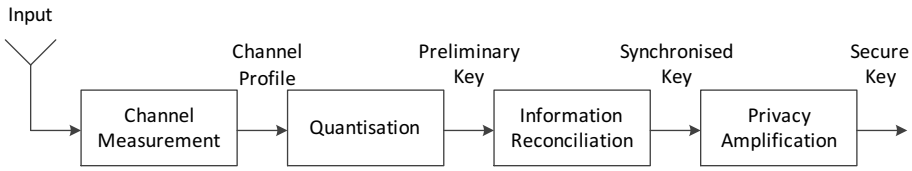

Figure 4.3: Standard Method of Key Generation.

a *synchronised key*. During the reconciliation process, the eavesdropper will also have access to the error detection and correction bits. Thus to minimise the possibility of key prediction, the security of the synchronised keys is enhanced in the privacy amplification stage to obtain a final *secure key*.

A detailed explanation of each step with appropriate references to the state of the art is given in the following subsection.

4.4.1 Channel Measurement

To construct the channel profile, the variations of the channel are measured at both the nodes within the coherence time of the channel. The various methods of constructing channel profile include;

1. Received Signal Strength Indicator(RSSI): RSSI is an indicator of the received signal strength at the receiver. It is usually used by wireless cards in laptops and sensor nodes, to measure the strength of the received signal w.r.t the base station or the transmitter. By measuring the variations of the RSSI, channel profiles are constructed in [51, 103, 12, 74].

   For wireless networks that experience a mobile channel, the variations in RSSI are easy to obtain. For wireless networks that experience a static channel, the variations can be obtained by using the frequency selectivity of the channel as done in [98, 99, 100, 66, 67].

   The primary advantage of RSSI measurements is that they can be easily measured using off the shelf wireless cards. They are usually measured

with the help of tools such as *iw*[48]. They don't need either any kind of special hardware or any modification to the wireless cards.

2. Impulse Response of Channel: Channel profile can also be constructed by estimating the impulse response of the channel [90]. The estimate can include the number of multi-paths, the coefficients of amplitude, and the phase of the channel. In [41, 57], phase estimates of the channel are used in building the channel profile.

   The channel estimation methods can impact the effectiveness of channel profile. Better channel estimation methods can yield better channel profiles.

3. Deep fades of received signal: Channel Profiles can also be constructed by estimating the deep fades of the received signal [82]. However as mentioned in [82], a special narrow band filter is necessary to measure the deep fades.

4.4.2 Quantisation

The channel profile is quantised into vector bits to obtain a *preliminary key*. Quantisation can be done either on the whole block of the profile or on smaller blocks of profile. They are broadly divided into *lossy* and *lossless* quantisation.

1. Lossless Quantisation: In lossless quantisation all measurements of the channel profile are considered. This type of quantisation usually has a single threshold. Values above the threshold are denoted as $+1$ and those below are -1. The threshold is usually the mean or the median of the channel profile. Examples of lossless quantisers are binary quantiser [12] and median quantiser[85].

2. Lossy Quantisation: In this type, multiple thresholds are considered. Values above and below the threshold, are usually assigned binary values according to Gray coding. While values between the threshold are usually discarded. The different methods of lossy quantisation include;

(a) Radio-Telepathy [65]

(b) Adaptive Secret Bit Generation(ASBG)[51]

(c) Multi-bit Adaptive Quantisation(MAQ)[74]

(d) Channel Quantisation with Guard-band(CQG)[94]

(e) Multi-level quantisation[98, 100, 66, 67].

4.4.3 Information Reconciliation

The preliminary key obtained at both the nodes are usually not identical. Due to noise, variations in channel measurement and variation in hardware, these errors in preliminary key exist. However without a synchronised key, encryption-decryption of the data is not possible. Hence to detect and correct the errors, reconciliation is done.

During this process, one of the node (e.g. Alice) generates the parity bits (error detection or/and error correction bits) of the preliminary key. Only the parity bits are transmitted to the other node (e.g. Bob). Using the parity bits and its (Bob's) preliminary key, Bob computes the preliminary key of Alice and obtains a synchronised key. The various methods of information reconciliation are:

1. Convolution codes [59]
2. Turbo codes [14]
3. Cyclic Redundancy Check(CRC) bits [75]
4. Low Density Parity Check(LDPC) codes [37, 76, 47, 64, 63, 62, 102]
5. Bose Chaudhuri Hocquenghem (BCH) codes [16, 55]
6. Key consistency algorithms [62, 103, 36]
7. Hash functions[56, 98, 100, 66, 67]
8. Fuzzy logic [29, 82]

9. Cryptographic techniques like secure sketch [78], and Cascade protocol[51, 17]

This process can be computationally intensive while detecting and correcting the erroneous bits. Hence by moving the computationally intensive process to nodes with higher processing power, such as base stations, the complexity can be appropriately distributed.

4.4.4 Privacy Amplification

During the reconciliation phase, the eavesdropper also has access to parity bits. To minimise the possibilities of key prediction, the security of the synchronised key is enhanced by privacy amplification. It can be done by various methods such as;

1. Secure hashes like SHA-1[72]
2. Fuzzy extractors[31, 78, 53, 30]
3. Pseudo-random generators from one-way function[38, 51]

4.5 Evaluation Metrics

In order to validate the effectiveness of the key generation methods, a set of metrics is necessary. Various metrics used in the state of art are;

1. **Bit Disagreement Rate(BDR)**: BDR indicates the percentage of bits that are in disagreement between the preliminary keywords of Alice and Bob. A higher BDR, indicates higher number of bits in disagreement in a preliminary key, there by increasing the effort needed to synchronise them. A lower BDR indicates, greater percentage of bits in agreement, thereby decreasing the effort needed to synchronise.

For example, with a lower BDR only error detection methods like CRC can be employed. This would not only decrease the complexity of the system but would also increase the system entropy.

2. **Key Generation Rate(KGR)**: The key generation rate indicates the number of secret key bits generated per second after quantisation. A higher bit rate indicates a longer key can be generated in a shorter period of time. This is essential since longer keys have higher entropy. A scheme with higher KGR can generate higher entropy keys.

3. **Randomness test**: This indicates the randomness of the key. In order that the keys generated be secure they must qualify the randomness test, since a random key is harder to predict and hence break the encryption. The keys can be tested for their randomness using various methods like the randomness test [35], the NIST test [72], and Muerer's statistical test [68].

   The NIST test can be conducted by using the NIST tool. It includes calculating a p value for different parameters such as; Frequency, Runs, Serial, Entropy, Cumulative sums, and Discrete Fourier Transform(DFT). If ($p \geq 0.01$) for every parameter, then the key passes the randomness test. In this thesis the NIST tool has been used to test the randomness of the secret key.

4. **Testbed**: As much as the performance of the key generation scheme depends on the channel measurement and quantisation schemes, it's performance also depends on the kind of the testbed used to generate the secret keys.

   A testbed simulating the real-world parameters can yield metrics that will not only be useful in developing better schemes of key generation, but also will be very helpful in deployment. Since a testbed consisting of nodes in a favourable environment(like line-of-sight conditions only) could yield better metrics on the experimental testbed, but when deployed in the real world,

their performance could be adversely effected. Hence it is very important to test the key generation schemes on testbed that reflect real world channel conditions like non line-of-sight conditions, multi-path propagation, and mobility, among the nodes of the network.

In this thesis, construction of such test-beds that reflect real world channel conditions have been developed and will be discussed in detail in the next chapter.

4.6 Need for Better Methods

Secret key management system exploiting the fading characteristics of the multi-path channel is a novel idea. A very effective deployment of such key management system can be achieved in mobile and vehicular ad-hoc networks. However for such a deployment, proper design and implementation strategies is necessary. The existing state of the art have thoroughly investigated all possible methods for each block of the key generation scheme, as seen in the previous section. A lot of possibilities exist, leading to a lot of variations. For effective deployment, it is essential to outline proper design parameters and adopt suitable methods of; channel measurement, quantisation, information reconciliation, and privacy amplification. Then suitable metrics and appropriate testbeds need to be adopted for a proper validation of the key generation scheme. However certain limitations do exist in the current methods such as;

1. In most of the work a single point baseline architecture as shown in Figure 4.3 does not exist. Such a structure is an essential starting point for developing better methods.

2. Most of the methods directly quantise the channel profile. Methods that can enhance channel reciprocity is one area that needs a deeper enquiry, since reciprocity enhancement methods can increase the performance of the system.

3. The channel measurements considered in most of the current methods are either drawn from statistical simulation models [47, 94] or they use specialised hardware like ESPAR antenna [12], directional antennas [45], array antennas[85], narrowband filters [82]. A testbed setup based on existing hardware that can yield, real-world channel measurements can be highly beneficial in validating the proof of concept.

4. Finally appropriate architecture for key management system and its corresponding deployment scenarios need to be also explored.

Given the above limitations we can deduce that the methods proposed in the state of the art are a good starting point in developing physical layer security. However to improvise on the existing implementation the following objectives can be proposed namely;

1. Introduce a common baseline model for key generation scheme.

2. Investigate various reciprocity enhancement methods in order to improve the BDR and KGR rates.

3. Validate the proposed key generation schemes using testbeds that provide real world channel measurements.

4. Finally propose suitable architecture and deployment use-cases for effective implementation of key management system.

It is these objectives that are thoroughly investigated in the next chapter.

4.7 Summary

To summarise, systems like mobile and vehicular ad-hoc networks will be deployed in large numbers in the future. Security of such networks is a necessary condition to be met for a successful deployment. Secret key management systems are an integral part of any security infrastructure.

By using the inherent fading characteristic of the wireless channel, a shared secret key between a pair of nodes can be established. The process consists of measuring the channel profile, quantifying it to get preliminary keys, synchronising it, before finally obtaining a secure key. By covering different variety of key generation methods, the various methods explored in the state of the art and their performance have been extensively discussed in the chapter.

As seen in the previous section, existing methods give a good starting point in building key management systems. However scope for improving the key generation process does exists. By systematically designing each block, an efficient scheme of key generation can be developed.

Key objectives in building key management systems include; building effective channel profiles, enhancing the reciprocity of the channel profile, and adaptive quantisation algorithms. To validate these schemes, it is equally important to test them on testbeds that reflect the real world channel measurements. Once such scheme is developed, an appropriate architecture and deployment strategies must be also explored. It is these objectives that are discussed in the next chapter.

Chapter 5

Improved Methods of Secret Key Generation

5.1 Introduction

Establishing shared secret keys using reciprocal and random variations of wireless channel, is a novel idea for deploying key management systems in wireless ad-hoc networks. However several limitations as discussed in the previous chapter, need improvements for effective deployments. Based on these limitations, the following objectives are investigated in detail in this chapter. These objectives are also the main contributions of the thesis, in the physical layer security section. The main objectives are:

1. A baseline model clearly depicting every stage of the key generation scheme. This includes from measuring the channel within the coherence time to, generating synchronised and secure keys.

2. Investigate various reciprocity enhancement methods in order to improve the performance of key generation. Most of the existing methods directly quantise the raw channel profiles. By processing the channel profile, its reciprocity can be improved.

By enhancing the reciprocity, the BDR and KGR rates of the preliminary key and hence the performance of key generation can be improved. Hence methods that can enhance the reciprocity of channel profiles are investigated.

3. The enhanced channel profiles must be quantised appropriately in order to efficiently generate preliminary keys. Hence quantisation schemes for enhanced channel profiles are also investigated.

4. Suitable key management architectures and deployment use-cases are proposed. This is necessary to give an initial idea of deployment of physical layer security in wireless ad-hoc networks.

5. Finally a proof of concept for the proposed key generation schemes is built by validating the schemes on testbeds that reflect real world channel measurements.

The organisation of the chapter is as follows. In Section 5.2 the various methods of reciprocity enhancement methods are discussed in detail. Then the methods of information reconciliation and privacy amplification are also discussed. Section 5.3 deals with the architecture of deploying physical layer security in mobile and vehicular ad-hoc networks. In Section 5.4 strategies for deploying physical layer security are discussed. The emphasis is on deploying key management systems for vehicular communication. Finally the main contributions of the chapter are summarised in Section 5.5.

5.2 Enhancing Channel Reciprocity

By employing specialized hardware like ESPAR antenna [12], directional antennas [45], array antennas[85], and narrowband filters [82], precise channel profiles can be measured. However general purpose hardware like wireless cards, cannot match the precision offered by the specialised hardware. Due to variations in

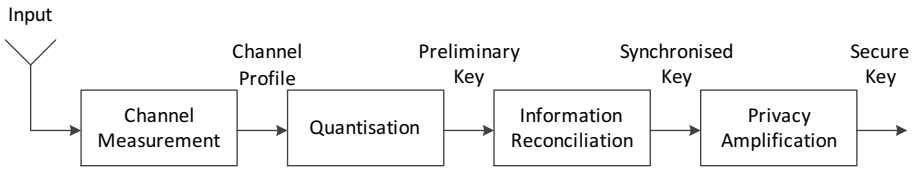

Figure 5.1: Standard Method of Key Generation.

hardware, noise, and half-duplex nature of the transceivers, it is not possible to construct channel profiles with exact reciprocities.

In the state of the art, most methods directly quantise the channel profiles as seen from Fig. 5.1. However by processing the channel profiles as shown in Fig. 5.2 enhancement in the reciprocity of channel profiles could be achieved. This enhancement in reciprocity can improve the performance of key generation. So in this section, different methods that enhance the channel reciprocity are examined. The different methods are:

1. l_1-norm minimisation
2. Hierarchical Clustering
3. Kalman Filtering
4. Polynomial Regression

5.2.1 Notations

To begin with certain set of notations are introduced. These notations are used in the forthcoming sections describing the methods of channel reciprocity enhancement, quantisation, information reconciliation, and privacy amplification.

Let Y be the channel profile, x be the enhanced channel profile obtained after enhancing the reciprocity. Let Key_{prelim} be the preliminary keys obtained after quantisation, P be the parity bits used for reconciliation, Key_{sync} be the synchronised keys after information reconciliation, and Key_{sec} be the secure keys ob-

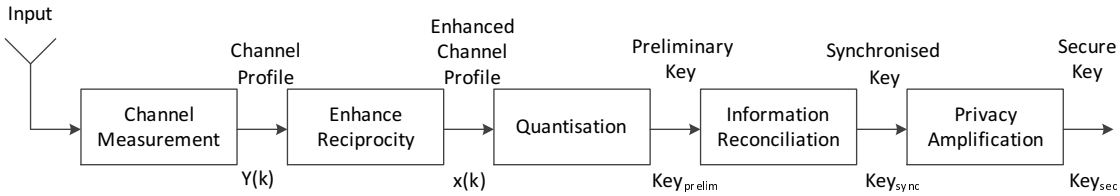

Figure 5.2: Enhanced Method of Key Generation.

tained after privacy amplification. The baseline model following these notations is indicated in Fig. 5.2.

In the following sub-sections, 4 methods of key generation are introduced, their abbreviations are as follows:

1. Key Generation by Enhanced Channel Reciprocity(KGECR)
2. Hierarchical Clustering based Key Generation(HCKG)
3. Kalman Filtering based Key Generation(KFKG)
4. Curve Fitting based Key Generation(CFKG)

5.2.2 l_1-norm minimisation

The first method of enhancing reciprocity is the l_1-norm minimisation [5, 58]. l_1-norm minimisation is widely used in solving under-determined system of linear equations. An under-determined system of linear equations usually has more unknowns than equations. Such a system can have infinite number of solutions. However if a sparse solution exists then it can be determined by using techniques such as the Greedy algorithm and linear programming [32].

Let the channel profile Y be obtained from the unknown vectors x such that:

$$Y = Ax \tag{5.1}$$

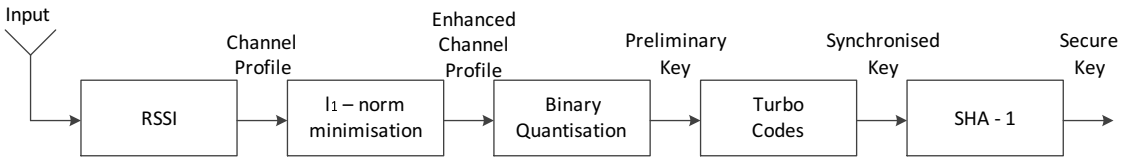

Figure 5.3: Enhancing Reciprocity through l1-norm minimisation(KGECR).

where, A is a $K \times N$ sensing matrix($K < N$)[43]. To recover x, an initial approximation vector x_0 is obtained such that

$$x_0 = A'Y \tag{5.2}$$

where A' is the transpose of A. The vector x is recovered from x_0 by applying a l_1-norm minimization[19, 20] on it such that:

$$min_{x \in R^n} \; ||x||_1 \; subject \; to \; Y = Ax \tag{5.3}$$

The recovered vector x is the enhanced channel profile. The matrix A, used in recovering the signal of interest is known as the sensing matrix.

Sensing Matrix: The matrix A is a sensing matrix if it satisfies the following set of properties:

1. Restricted Isometry Property(RIP): The matrix A satisfies the RIP property [43] if all of its sub-matrices A_s are subjected to the condition

$$(1 - \delta_s)||y||_{l_2}^2 \leq ||A_s y||_{l_2}^2 \leq (1 + \delta_s)||y||_{l_2}^2 \tag{5.4}$$

   where $\delta_s \in (0, 1)$ is the RIP constant and $y \in R^n$.

2. Incoherence: The incoherence of the matrix A is defined as

$$\mu = max_{j>k} \frac{|< A_j, A_k >|}{||A_j||_2 ||A_k||_2} \tag{5.5}$$

The property of incoherence is to ensure that columns of matrix A are uncorrelated.

3. Orthogonality: The rows of the sensing matrix A must be orthogonal to each other such that

$$< A_j, A_k > = 0 \tag{5.6}$$

where A_j and A_k represent the jth and kth rows of matrix.

Toeplitz Random Sensing Matrix: An example of sensing matrix is the Toeplitz random sensing matrix [43]. They satisfy all the above mentioned property and are also easy for hardware implementation. They are constructed by using one of the following distributions:

- $r_i \sim unif[-\sqrt{3/\epsilon}, \sqrt{3/\epsilon}]$
- $r_i \sim \begin{cases} \frac{1}{\sqrt{\epsilon}}, & \text{with prob. } 1/2 \\ -1/\sqrt{\epsilon}, & \text{with prob. } 1/2 \end{cases}$
- $r_i \sim \begin{cases} 1/\sqrt{\epsilon q}, & \text{with prob. } q/2 \\ 0, prob.(1-q), q \in (0,1) & \\ -1/\sqrt{\epsilon q}, & \text{with prob. } 1/2 \end{cases}$

where, $\epsilon = k$ for partial matrix, $\epsilon = p$ for full matrix, and $p = n + k - 1$, $(k \geq n)$. Once the matrix is constructed the rows are orthogonalised to satisfy the orthogonality property.

Binary Quantisation: The enhanced channel profile x is quantised using the method of binary quantisation. The lossless binary quantizer consists of a single threshold. Values above the threshold are allocated a 1 and those below it a 0 as shown in Fig. 5.4. The threshold is the mean of all the values of the enhanced channel profile.

Thus in KGECR method the channel profile is enhanced by using l_1-norm minimisation and the preliminary keys are generated using the binary quantiser.

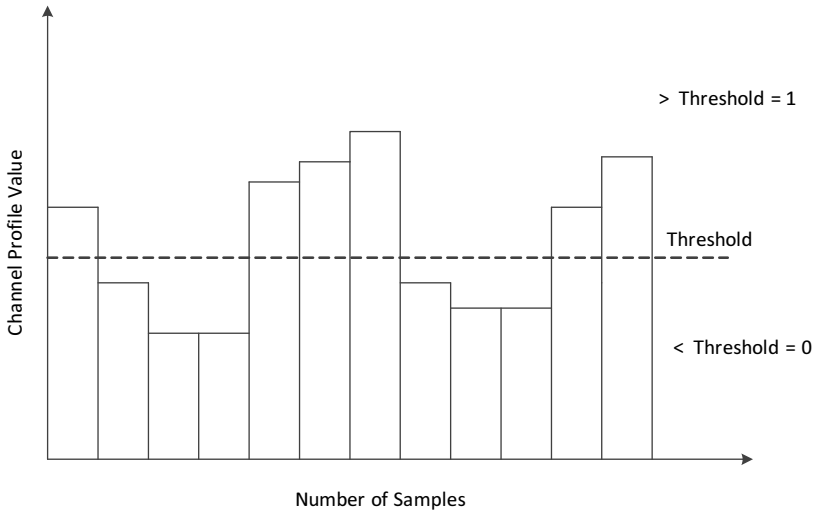

Figure 5.4: Binary Quantisation.

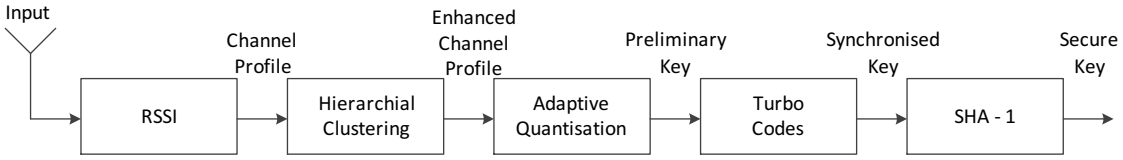

Figure 5.5: Enhancing Reciprocity through Hierarchical Clustering(HCKG).

5.2.3 Hierarchical Clustering

The second method of enhancing reciprocity is the hierarchical clustering. Hierarchical clustering is a method of clustering data points. By aggregating consecutive pair of data points to form a new data point clustering can be achieved. The purpose of clustering is to smoothen out irregular variations in the data. The aggregation of the data is done by either taking the mean or median of the consecutive points.

So in order to enhance the reciprocity, the consecutive data points of the channel profile are aggregated to obtain a smoothened channel profile. The enhanced profile has better reciprocity compared to the original profile. However a disad-

vantage is that the number of data points halve for every level of clustering thereby decreasing the key generation rate by a factor of 2 for every hierarchy. Hence in order to avoid a drastic reduction in key generation rate, hierarchical clustering consisting of a single level is used. The enhanced channel profile is quantised using an adaptive quantisation.

Adaptive Quantisation

The adaptive quantisation consists of the following steps:

1. The channel profile is divided into blocks of size *Blocksize* and then processed according to different levels of quantisation. A blocksize of 10 always yields better performance.

2. Each level of quantization is based on the following relation:

   (a) level 1 = $[-\infty, \hat{m} - \frac{\sigma}{2}]$

   (b) level 2 = $[\hat{m} - \frac{\sigma}{2}, \hat{m}]$

   (c) level 3 = $[\ \hat{m}, \hat{m} + \frac{\sigma}{2}]$

   (d) level 4 = $[\hat{m} + \frac{\sigma}{2}, \infty]$

   where, $\hat{m}$ is the mean and σ is the variance of, the channel profile block. Gray coding is used to assign a binary codeword to each quantization level as shown in Fig. 5.6.

3. Alice transmits the positions that lie in quantization levels 1,3(00,11) and 2,4(01,10) respectively, to Bob. Bob sends an acknowledgement indicating the commonly agreed levels of quantization.

Even though Alice and Bob exchange the levels of quantization, Eve will not be able to compute the same values of level 1, 2, 3, and 4 since his mean and variance differ from that of Alice and Bob. Hence Eve cannot predict the preliminary key by knowing only the levels 1 to 4.

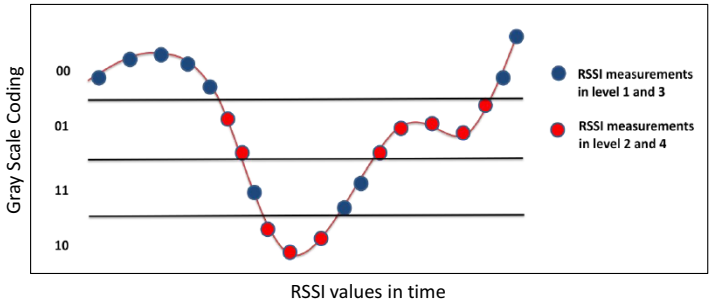

Figure 5.6: Adaptive Quantization.

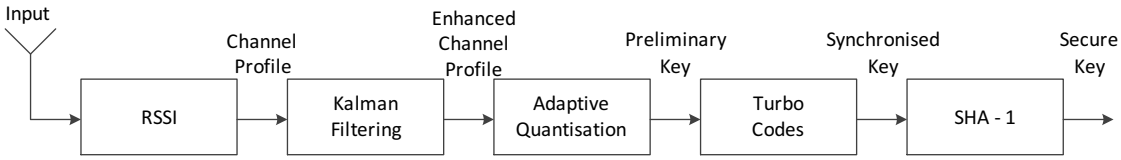

Figure 5.7: Enhancing Reciprocity through Kalman filtering(KFKG).

Thus in the HCKG method, the channel profile is enhanced by using the method of hierarchical clustering and, preliminary keys are generated using the method of adaptive quantisation.

5.2.4 Kalman Filtering

Kalman filter is the third method used for enhancing channel reciprocity [10]. Kalman filter also known as linear quadratic estimation, was first described in technical papers by Swerling in 1958, Rudolf Kalman in 1960, and Kalman and Bucy in 1961. It is a a set of mathematical equations that recursively estimates the state of a process such that, the mean of the squared error is minimised [95]. It can estimate past, present, and future estimates of a process even without an accurate knowledge of the system being modeled. Thus it is used in various applications like navigation, missile guidance and control, signal processing applications, and even in stock market estimations.

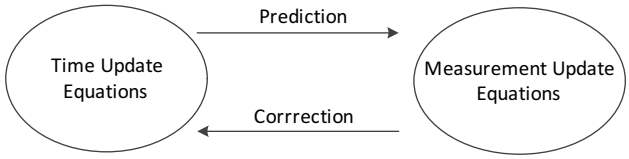

Figure 5.8: Recursive Iteration between Time and Measurement Update Equations.

The parameters of a system are recursively estimated by using apriori and aposterio estimations. The initial prediction of channel profile is done in time update equations. The predicted estimation is corrected in the measurement update equations. As shown in Fig. 5.8 by recursively estimating between time and measurement update equations, the channel profile values are estimated to obtain an enhanced channel channel profile.

Let x_k be the estimated channel profile and y_k be the measured channel profile such that [95],

$$x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1} \tag{5.7}$$

where A is $n \times n$ matrix representing the state at time $k-1$, B is a $n \times l$ matrix representing the optional control input $u \in R^l$, and w_k is the process noise.

$$y_k = Hx_k + v_k \tag{5.8}$$

where H is the $m \times n$ matrix indicating the state of measurement at time k and v_k is the measurement noise.
The normal probability distribution of process and measurement noise is given by;

$$p(w) \sim N(0, Q) \tag{5.9}$$

$$p(v) \sim N(0, R)$$

where Q and R are the process and measurement noise co-variance respectively.

Let $\hat{x}_k^-$ be the apriori estimation and $\hat{x}_k$ be the aposteriori estimation of the channel profile then the errors during the estimation can be defined as;

$$e_k^- = x_k - \hat{x}_k^- \tag{5.10}$$

$$e_k = x_k - \hat{x}_k$$

where e_k^- and e_k are the apriori and aposteriori estimate errors respectively. Their respective error co-variance being;

$$P_k^- = E[e_k^- e_k^{-T}] \tag{5.11}$$

$$P_k = E[e_k e_k^T]$$

The enhanced channel profile are estimated through a recursion between the time update and measurement update equations.

The time update equations used to predict the channel profile are:

$$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \tag{5.12}$$

$$P_k^- = AP_{k-1}A^T + Q$$

While the measurement update equations used to correct the apriori estimated channel profile are:

$$K_k = \frac{P_k^- H^T}{(HP_k^- H^T + R)} \tag{5.13}$$

$$\hat{x}_k = \hat{x}_k^- + K(y_k - H\hat{x}_k^-)$$

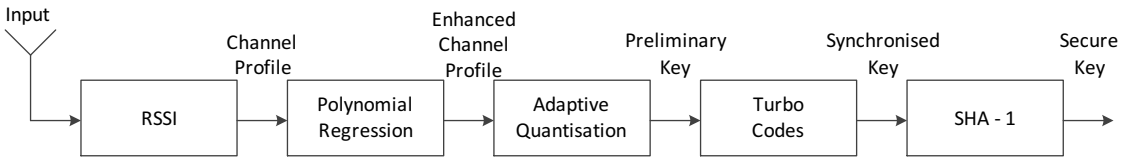

Figure 5.9: Enhancing Reciprocity through Polynomial Regression(CFKG).

$$P_k = (I - K_k H)P_k^-$$

where, K_k is referred to as the Kalman gain.

Thus in the KFKG method, Kalman filter is used to estimate the enhanced channel profile. The enhanced profile is further quantised using the method of adaptive quantisation.

5.2.5 Polynomial Regression

The fourth method of enhancing channel reciprocity is polynomial regression. Polynomial regression is a method of fitting a curve to a random set of data. It belongs to the regression class of algorithms. The main objective is to describe a polynomial function in time that best describes the rate of change of the random samples.

Hence the method of enhancing reciprocity by polynomial regression is to curve fit the random variations of the channel profile and obtain an appropriate polynomial. The coefficients of the polynomial indicate the rate of change of the channel profile variations. Hence it is the rate of change of channel profile that describes the enhanced channel profile.

For a given channel profile, let the independent variable x_i be time and the dependent variable y_i be the channel profile measurements. The polynomial expression representing the rate of change of random samples will be [4, 42]:

$$y_i = a_0 + a_1 x_i + a_2 x_i^2 + \ldots + a_m x_i^m + \epsilon_i \tag{5.14}$$

where $i = (1, 2, \ldots, n)$, y_i indicates the channel profile at time x_i and ϵ_i is the difference in the measurements of channel profile. Hence the polynomial that best fits the channel profile measurement is $a_0 + a_1 x_i + a_2 x_i^2 + \ldots + a_m x_i^m$ and $a_0, a_1, \ldots, a_m$ are the coefficients of the polynomial that represent the rate of change of the profile. The curve fit profile is the enhanced channel profile.

Thus the CFKG method enhances reciprocity by curve fitting the random variation of the channel profile and then quantises the enhanced profile by using the method of adaptive quantisation.

5.2.6 Information Reconciliation and Privacy Amplification

The disagreeing bits of the preliminary keys are detected and corrected in the information reconciliation stage as indicated in Fig. 5.2. Turbo Codes [14] are used to detect and correct the disagreeing bits of the preliminary key. Bob calculates the parity and tail bits for his preliminary key. Only the parity and tail bits are transmitted to Alice. Alice receives the parity and tail bits, and detects and corrects the disagreeing bits to obtain the preliminary key of Bob thereby synchronising it.

Let K_A and K_B be the preliminary keys of Alice and Bob respectively. Let P_B be the parity and tail bits calculated by Bob. Then Alice recovers the preliminary key K_B using the parity bits P_B through a Turbo decoder. Thus both Alice and Bob reconciliate for the same key K_B by using the Turbo decoder.

During information reconciliation, the parity bits transmitted through the wireless channel are also available to the eavesdropper. Hence to minimise the possibilities of key prediction the bits of the synchronised key are de-correlated during the privacy amplification stage. As described in the previous chapter, privacy amplification can be done using different methods such as; one-way functions, fuzzy extractors, and secure hashes.

In this thesis the SHA-1 [72] secure hashes are used for the privacy amplification stage. SHA-1 is a one-way cryptographic hash function that produces a 160-bit secure hash. It was designed by the United States National Security Agency as a Federal Information Processing Standard. One way functions are functions wherein a corresponding output is generated from a given input. However the input cannot be predicted by using the output hence the name one-way functions. It also has the avalanche property i.e. a slight change in the input produces a completely different result. This property greatly enhances the security of the secure key since any change in single bit of the input key drastically changes the final secure key.

The topic of information reconciliation and privacy amplification are not the main objectives of the thesis. In order to build a complete system of key generation, information reconciliation and privacy amplification methods have been implemented with the methods present in the state of the art. For reconciliation the Turbo codes of the IT++ tool are used. While for SHA-1, the matlab code available at NIST [72] is used to derive the SHA-1 secure hashes.

5.3 Architecture: KeyBunch

To effectively deploy key management system in wireless ad-hoc networks, it is essential to have an architecture. Since an architecture can help in design, planning and a subsequent deployment of key management systems. To thoroughly exploit the fading characteristics of the wireless channel an architecture *KeyBunch* is proposed.

The objective of KeyBunch is to exploit all possible characteristic of the wireless channel and extract, synchronised and secure secret keys, to make it available to the application layer (for encryption and decryption) in real time. The functional block diagram of KeyBunch is as shown in Fig. 5.10.

The main functions of KeyBunch are:

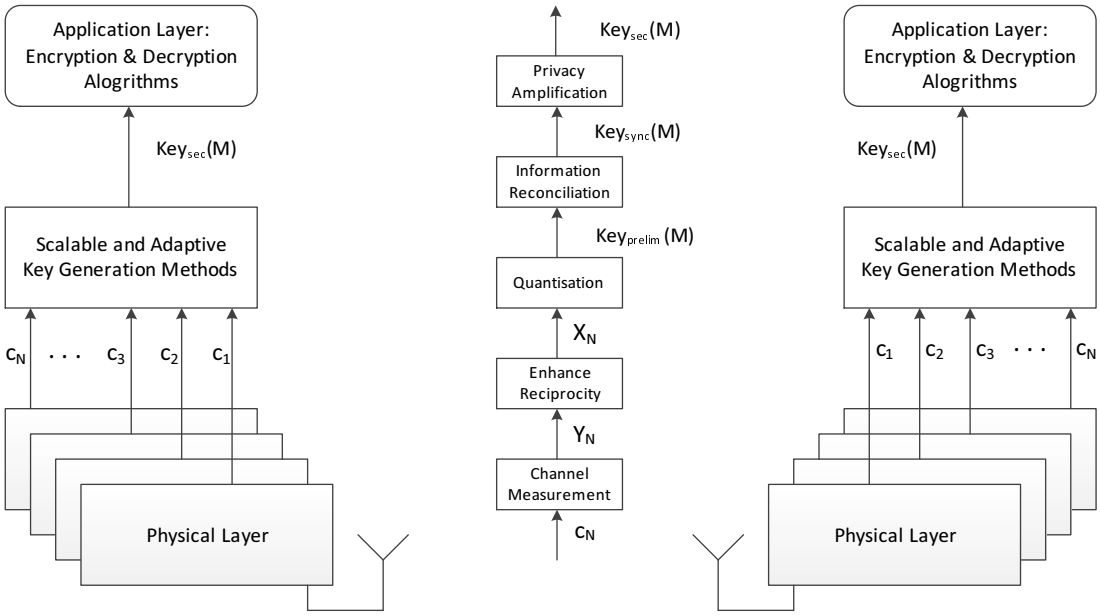

Figure 5.10: KeyBunch:Key Management in Ad-hoc Networks

1. A channel profile C_N is built by measuring the channel in N different methods.

   The different channel measurements can include: RSSI profiles, impulse response of the channel, phase estimates, or deep fades of the received signal as discussed in the previous chapter. The purpose of including different methods of channel measurements is to ensure a high degree of system entropy. Moreover different methods of channel measurement can provide different random sources for key generation.

2. The channel profiles C_N are quantized to obtain the preliminary set of keys $Key_{prelim}(M)$, where $M = N \times P$ and P is the number of quantization algorithms considered for quantising the profiles. The quantisation on the set of channel profiles C_N can be done in two ways.

   In the first method, if only a single method of channel measurement (e.g.

RSSI) is possible then, different quantisation schemes can be employed on the same channel profile. Since several quantisation schemes use different threshold parameters, mutually exclusive preliminary keys $Key_{prelim}(M)$ can be obtained on the same profile. For example, different quantization algorithms based on RSSI have been proposed in [51, 74, 12, 5, 4]. These algorithms can be used on the same RSSI profile to generate different sets of preliminary keys.

For the second method, a device that can record multiple methods of channel measurement, different methods of quantization [94, 65, 51, 74, 98, 12, 5, 4] can be employed. This will also certainly yield different preliminary keys.

3. The errors present in preliminary keys can be detected and corrected by using the various methods of information reconciliation as discussed in the previous chapter such as Turbo codes, Cascade protocol, LDPC codes etc. Thus a synchronised bunch of keys $Key_{sync}(M)$ is obtained.

4. Finally the entropy of the synchronized keys is enhanced by various methods of privacy amplification to obtain a secure key-bunch $Key_{sec}(M)$.

Thus KeyBunch facilitates the extraction of synchronised and secure set of keys $Key_{sec}(M)$ by utilising the random variations from N different channel profiles. This method can be adopted in wireless ad-hoc network to satisfy the confidentiality attribute of security. Before the nodes generate KeyBunch it is essential that they commonly agree upon the parameters of N and P, i.e. the number and type of channel profiles and the number and type of quantisation algorithms. Hence an initial configuration of commonly agreed parameters is necessary. But once these parameters have been setup, secure key bunches can be established between peer-peer nodes of an wireless ad-hoc network.

5.4 Deployment Strategies

Recent methodologies such as the Internet-of-things (IOT), Machine to Machine Communication (M2M), Cyber Physical Systems (CPS) have got more recognition from both industry and academia. Be it in terms of ideas, concepts, projects, products, and a viable roadmap for the future, significant efforts have been made in this direction. For instance a quick search on these topics in IEEE Xplore results in around 1800 results for IOT, 67000 for M2M, and nearly 1200 for CPS indicating interests in; envisioning future systems, applications, deployments, and business models.

Wireless communication technologies such as Personal Area Networking (PAN), Vehicular Communication (VC) or Car to Car communication, Wireless Sensor Networks (WSN), Mobile Communication Standards such as 2G, 3G, 4G, all come under the gambit of the above proposed systems. Envisioning and deploying such systems have been possible due to development in both sensor and communication technologies.

For a successful deployment of these systems it is necessary that the attributes of security must be met. For it is security that will allow a seamless and non-intrusive connectivity among the nodes of the network. As an use case scenario, the security in Vehicular Communications (VC) is considered in this section. The objective is to explore the possibility of key management in VC by applying the concepts of physical layer security.

The rapid growth of vehicles over the past decade has presented an abundance of problems related to road safety such as; an increase in accidents, traffic congestion, and pollution. These problems are bound to grow over time with an ever increasing growth of vehicles. Hence to deal with this situation and improve the condition of road safety and travel, the idea of VC has been envisioned. With significant advances in sensing and communication technologies, efforts are being made to introduce communication capabilities between vehicles such that road safety can be improved dramatically.

Vehicular communication aims at fostering road traffic management by pro-

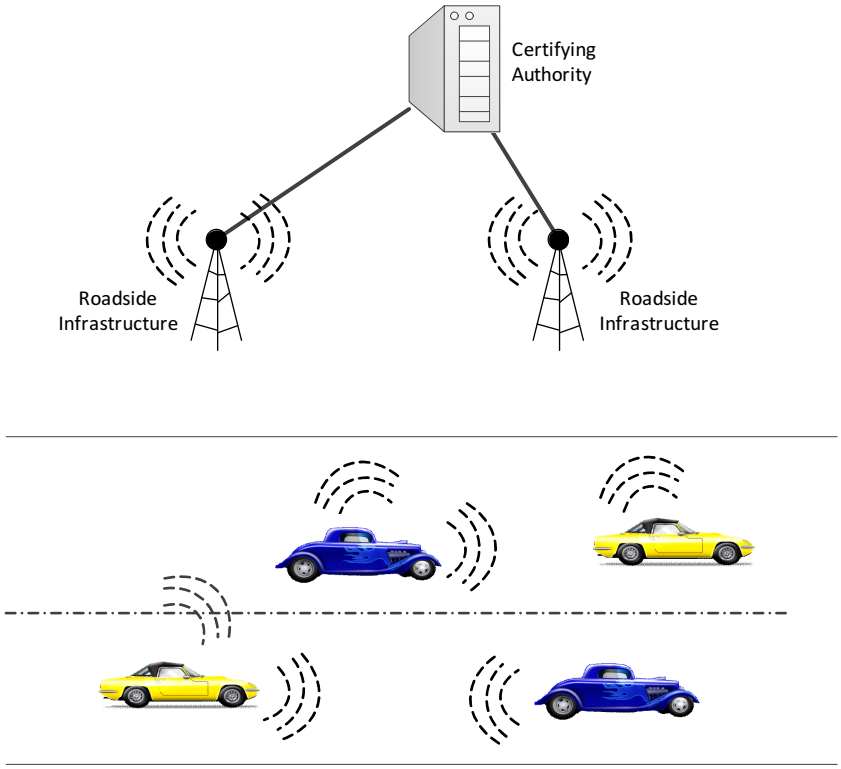

Figure 5.11: Securing Vehicular Communication.

viding real-time traffic management in terms of speed, congestion, weather patterns, emergency services, and tourist information. Availability of such services in real-time can thus significantly improve the safety and reliability of road transport.

The system model of VC can be as shown in Fig. 5.11. Vehicular communication consists mainly of vehicles on the road and road side infrastructure (RSI) off the road. Equipped with onboard sensors and communication equipment, communication can happen between both vehicle to vehicle (V2V) and vehicle to road side infrastructures (V2RSI).

In order to fulfill the objectives of security in VC, the *Secure Vehicle Communication* (Sevecom) consortium [28] was founded by an industry-academia collaboration. It mainly focusses on providing a baseline architecture for security as-

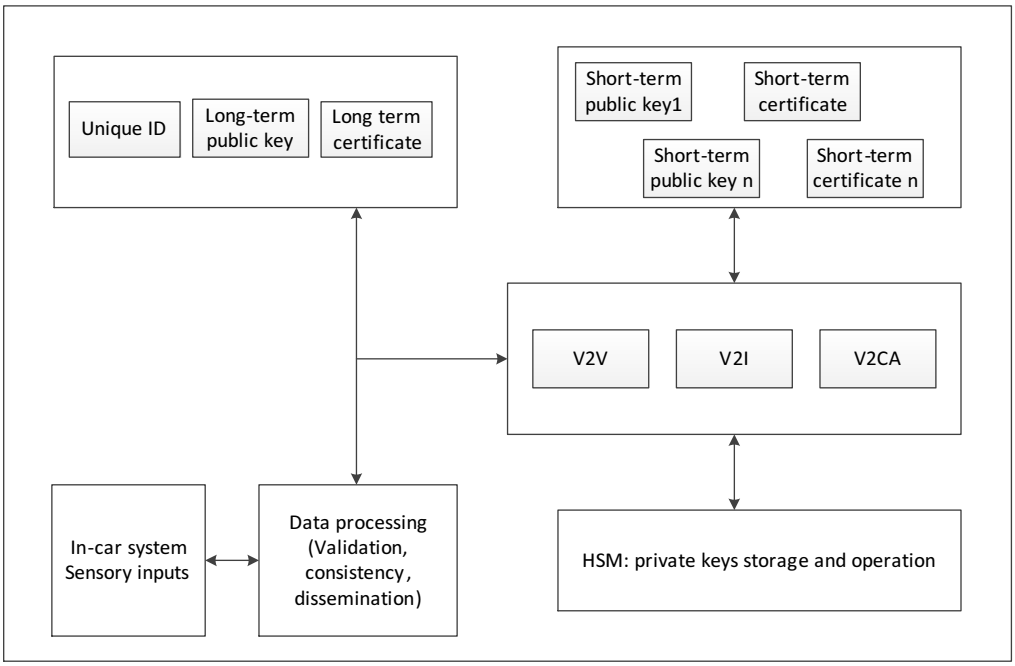

Figure 5.12: Baseline architecture for Sevecom.

pects in VC such as; identity, cryptographic management, privacy protection, secure communication, and in-car protection [73]. The baseline architecture aimed at both the vehicles and road side infrastructure units (RSUs) is shown in Fig. 5.12.

5.4.1 Secure Vehicular Communication(Sevecom)

Since the main focus is on key management system the other attributes of Sevecom are not discussed here. Only the aspects of key management in VC are of main interest. The module that addresses the key management attribute of VC is the Hardware Security Module (HSM) [73] as shown in Fig. 5.12.

The main objective of HSM is to store sensitive information and provide a secure time base. It is responsible for the confidentiality of the communication happening between V2V and V2RSI and is the, main basis of trust. It hosts a set of

secret keys that are used for decryption of data. An initial set of keys are installed during initial installation. Further long-term updates of the keys are issued by the Certifying Authorities (CAs) for lifelong maintenance.

The HSM consists of a CPU, a non-volatile memory, an inbuilt clock and an I/O interface. Thus its functionalities can be implemented as a SOC. It also has a built-in battery, a tamper detection and reaction circuitry. Any tampering of the HSM module leads to erasure of the private keys thereby preventing any form of secret key extraction.

Porting KeyBunch to Sevecom

The HSM modules of Sevecom has the following limitations that can be over come by implementing physical layer security. The limitations are:

1. Dependability for Keys: The HSM is always dependent on an external authority for the supply of secret keys. This dependency is an overhead and also a weak link for the system security. Instead an autonomous system of key management where the nodes can independently manage keys is necessary.

2. Points of Compromise: The keys installed on the HSM can be compromised at various points such as during initial installation, long-term update by CAs or during servicing of the vehicles at garages. Stolen secret keys will eventually lead to a compromise in confidentiality of the vehicular network eventually making them vulnerable to attacks.

3. Lifelong Maintenance: The HSM comes with a set of pre-installed keys. These keys need to be updated periodically by the CAs in order to prevent any brute force attack. Hence an overhead of lifelong maintenance of the secret keys is always present.

4. HSM Tampering: The HSM is always at a risk of being tampered with. For instance the HSM can be tampered with during the servicing of the vehicle.

Therefore tamper detection and reaction circuitry are necessary.

The above listed limitations can be overcome by deploying KeyBunch based SOC implementation into the HSM [6]. By doing so, the following advantages can be realised:

1. Autonomous Key Generation: Both the Vehicles and RSI will be empowered to independently generate their own keys. Dependency on an external authority will not exist since all keys will be generated by using the random and reciprocal variations of the wireless channel in real-time.

   Hence a *Plug & Secure* approach for key management can be realised in the HSM module of the Sevecom architecture.

2. Compromise Proof: Since all keys will be generated independently and in real-time, the points of compromise and the need for lifelong maintenance will not exist.

3. Tamper Proof: All keys will be generated in real time hence no keys need be stored in the HSM. As a result, the risk of HSM tampering also does not exist.

4. Enhanced Security: With the KeyBunch, multiple sets of keys(instead of a single key) can be generated. This can eventually be used in various configurations to enhance system security. For instance, either the entire KeyBunch can be used or a different key from the KeyBunch can be used per session, for establishing confidentiality between nodes. This will drastically increase the effort needed to break the key through a brute force attack thereby enhancing the security.

Thus by exploiting the random and reciprocal variations of the wireless channel, KeyBunches can be established between vehicles-to-vehicles(V2V) and vehicles to road side infrastructure(V2RSI).

5.5 Summary

Improved methods of key generation schemes utilising the random and reciprocal variations of the wireless channel have been discussed in this chapter. The main objectives that were covered are:

1. A baseline architecture model clearly depicting the four stages of key generation. The four stages discussed and implemented include; channel measurement, quantisation, information reconciliation, and privacy amplification.

2. A fifth stage namely *"enhance reciprocity"* is proposed to improve the key generation scheme. Various methods are used to process the channel profile and to enhance its reciprocity. They include:

   (a) l_1-norm minimisation

   (b) Hierarchical Clustering

   (c) Kalman Filtering

   (d) Polynomial Regression

3. The enhanced channel profiles are quantised appropriately. For the l_1-nom minimisation method a binary quantiser is used to generate the preliminary keys.

   While for the other three methods namely; Hierarchical Clustering, Kalman filtering and Polynomial regression, an adaptive quantisation is used.

4. The disagreeing bits of the preliminary keys are detected and corrected using Turbo codes to obtain a synchronised key.

5. To prevent any possibilities of key prediction, SHA-1 secure hashes of the synchronised key are generated to finally obtain, secure keys.

6. Based on the above mentioned five stages, four different methods of key generation have been proposed namely:
   (a) Key Generation by Enhanced Channel Reciprocity(KGECR)
   (b) Hierarchical Clustering based Key Generation(HCKG)
   (c) Kalman Filtering based Key Generation(KFKG)
   (d) Curve Fitting based Key Generation(CFKG)
7. An architecture *KeyBunch* that utilises all the characteristic of wireless channels and generates, synchronised and secure bunch of secret keys is proposed. The main advantage of KeyBunch is that instead of generating a single key, sets of secure keys can be generated by using either the same or multiple sources of wireless channel. This drastically enhances the system entropy.
8. As a usecase, the KeyBunch is deployed in Vehicular Communications to securely generate keys between vehicle to vehicle and vehicle to roadside infrastructure. By porting KeyBunch onto the HSM module it is shown that the system entropy of the vehicular communication can be enhanced.

Thus all the four main objectives described at the beginning of the chapter have been thoroughly discussed. In the next chapter, the fifth objective of validating the proposed schemes on a testbed yielding real world channel measurements and evaluating its performance is discussed in detail.

Chapter 6

Testbed and Performance Evaluation

The evaluation of improved methods of key generation proposed in the previous chapter using real-world channel measurements is done in this chapter. This chapter is organized as follows; in Section 6.1 the testbed comprising of MIMO setup and wireless cards is presented. In Section 6.2 the performance of the key generation is evaluated with focus on static networks, mobile ad-hoc networks, and vehicular ad-hoc networks. In Section 6.3, observations based on the results of performance evaluation are discussed. Finally the chapter is summarized in Section 6.4.

6.1 Testbed

Statistical channel models based on Rayleigh fading characteristics are usually used to model the behavior of wireless channels during software simulations. Such statistical models give a good approximation of the nature of fading and the Doppler effects on the transmitted signal. They are a good starting point in validating transmitter and receiver systems. However for effective deployment, a working proof-of-concept based on channel measurements from real world would

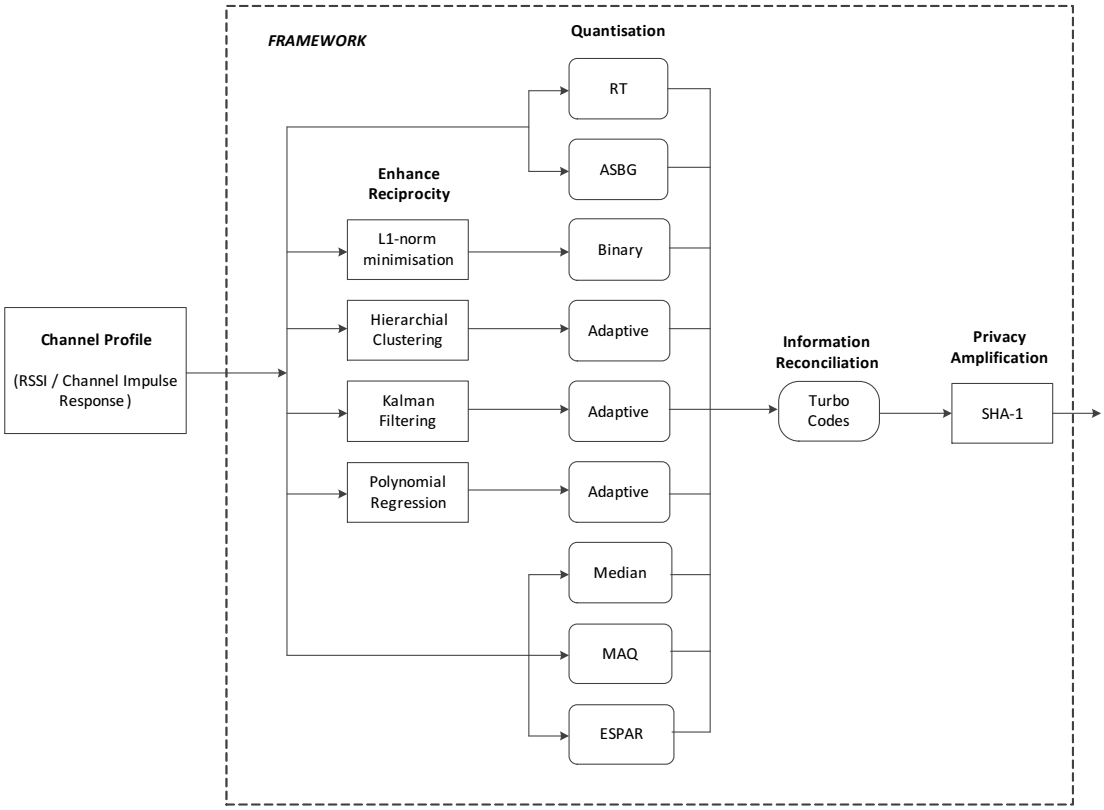

Figure 6.1: Framework for Key Generation.

be beneficial. Hence in order to develop proof-of-concepts, testbeds reflecting real world channel measurements are constructed and used for validation.

The testbeds include; 2x3 MIMO setup, IEEE 802.11 based wireless cards, and Universal Serial Radio Peripheral (USRP) based software defined radio. They cover three channel conditions namely; static networks, mobile ad-hoc networks, and vehicular ad-hoc networks.

In case of the setup consisting of MIMO link and wireless cards, the methodology is to build databases of channel profiles (RSSI) and process it offline, using the framework shown in Fig. 6.1. While in case of the USRP based setup, a real-time bi-directional key generation is demonstrated.

6.1.1 Static Networks

Given the wide deployment of static networks (e.g. wireless sensor networks), the problem of extracting secret keys in such networks is important. As the variations in static channels are relatively flat, it is difficult to extract secret keys. Hence methodologies for extracting keys in static networks need to be determined.

This work was a joint effort between Fraunhofer Heinrich Hertz Institute (HHI) Berlin and University of Kaiserslautern as part of the BMBF project *Prophylaxe*. HHI provided the 2x3 MIMO channel measurements through their MIMO testbed and the measurements were validated using the framework developed in this thesis as shown in Fig. 6.1. The main result of this collaboration was that by using frequency selectivity, extraction of keys in static networks can be done effectively.

System Setup

The measurement setup for the 2x3 MIMO network is shown in Fig. 6.2. It includes:

- A host computer to adjust the MIMO-transceiver to a desired configuration and to control the transmission process (with the Agilent software VEE).
- Five analog-to-digital and digital-to-analog boards within a common frame allowing a simultaneous trigger for all boards and hence a simultaneous transmission and reception. Two inputs and two outputs are used from each board yielding a maximum transmission rate of 250 kbit/s per port.
- The Insertion (6 HU x 1/2 19") contains five reciprocal transceiver with adjustable baseband amplification which are fully controllable via the host computer. Thereby, every transceiver can be switched in the transmit or receive mode independent of the other transceivers. Reciprocal transceivers are designed to allow an improved ad-hoc reciprocity [52].
- The LO for the MIMO-transceiver which consists of a commercial available synthesizer delivers a power of about 10 dBm at a frequency of about 5.2

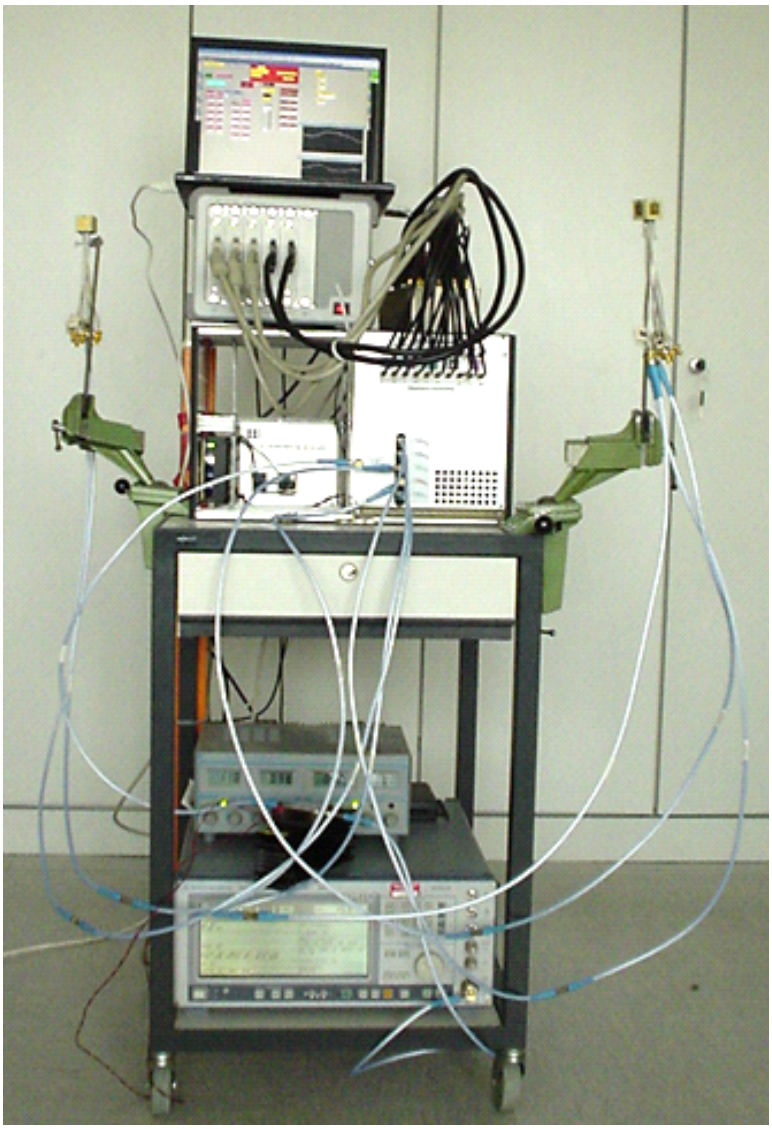

Figure 6.2: MIMO-TRx configured as 2x3-MIMO-System.

GHz to each transmitter. To allow frequency dependent channel measurements the LO frequency can be adjusted by the computer.

- Two cubic antennas, one at each side of the setup to avoid a LOS connection.

The antennas and the corresponding polarisations used are shown in Fig. 6.3.

As modulation different 128-bit long orthogonal Gold-series are applied to the transmitting antennas and transmitted simultaneously to the receive antennas. Then, the received signals are correlated with the transmitted Gold-series yielding separated channel characteristics.

Channel Measurements

The channel measurements estimated for the transceiver is as shown in Fig. 6.4. The RSSI [1] is calculated from the h parameters namely h_{11}, h_{12}, h_{21}, and h_{22} such that:

$$RSSI = 10 \cdot log_{10}(h_{11}^2 + h_{12}^2 + h_{21}^2 + h_{22}^2)$$

Four different channel conditions for the testbed are considered namely; Ch_a, Ch_b, Ch_c, and Ch_d. The characteristics of each channel is described as:

1. Ch_a: Measurements are conducted in the frequency range of 5.15 to 5.25 GHz. All measurements are conducted in an empty room, with each channel separated by 1/2 MHz to obtain 200 channels (sub-bands).

2. Ch_b: Measurements in the frequency range 5.15 to 5.25 GHz are conducted in the same room with two people. Each channel is separated by 1/3 MHz to obtain 300 channels.

3. Ch_c: Channel measurements in the frequency range of 5.19 to 5.21 GHz are conducted for a static channel with varying power level as shown in Fig. 6.5. Each channel is separated by 1/3 MHz to obtain 60 channels.

[1] Hardware manufacturer specified RSSI to have a measure of the mean received RF-power ($\sim$ dB) for using in the following baseband circuits [2]. Absolute accuracy of the RSSI reading is not specified as well as a linear operation over the total range. Here, RSSI is approached by the power of the channel measurements.

4. Ch_d: Channel measurements in the frequency range of 5.19 to 5.21 GHz are conducted for a static channel with varying positions. A total of 60 channels is obtained by separating them at 1/3 MHz.

The size of the room where the channel Ch_a, Ch_b, Ch_c, and Ch_d is measured is about 5 m x 8 m with a height of about 3 m.

6.1.2 Mobile Ad-hoc Networks

To simulate the conditions of moving networks, mobile ad-hoc networks are constructed using IEEE 802.11 based wireless cards. Wireless cards are transceiver front-ends that are usually built-in with all laptops. They are mainly used in connecting the client (such as laptops) to an access points (AP), to enable the clients, wireless fidelity and over the air access of Internet. These wireless cards can also be obtained as off-the-shelf hardware. Manufacturers of such wireless cards include, Intel, Atheros, and D-Link. They transmit and receive using Time Division Duplex (TDD) diversity in the ISM frequency band. RSSI is one of the parameters considered to connect clients to the nearest base station.

System Setup

In this thesis four laptops are considered for the testbed based on wireless cards. They are named as Alice, Bob, Eve, and Janet. Alice and Bob are the legitimate nodes. While Eve and Janet are the adversary nodes that passively eavesdrop on the communication happening between Alice and Bob. Alice is configured as the base station. While Bob, Eve, and Janet are configured as client.

All the four laptops have Ubuntu operating system installed. An utility tool known as "*iw*"[48] is used to measure the RSSI on each laptop. Alice is equipped with an Atheros wireless card while Bob, Eve, and Janet are all equipped with Intel Pro wireless cards. Wireless cards from different manufacturers are used, to ensure heterogeneity in RSSI measurements.

Alice always initiates the communication by transmitting pilot sequences. Upon initiation, Bob, Eve, and Janet acknowledge back by transmitting their pilot sequences. The communication happens in 2.4 GHz frequency in the ISM band. Bob is placed at a distance of 50 meters from Alice, while Eve is 20 meters away from both Alice and Bob, and Janet is 40 meters away from both Alice and Bob.

Channel Measurements

To simulate the channel conditions of a mobile ad-hoc network, Alice moves around, while Bob, Eve, and Janet are all kept stationary. Alice moves upto 200 meters from its starting point in order to obtain channel measurements that reflect non-line-of-sight conditions. The RSSI profiles are obtained by conducting the experiment in various channel conditions such as; Indoor lab, University Campus, Forest(near the University), and City Center.

The iw tool assists in measuring the RSSI values. A total of 75 RSSI measurements are recorded per profile. The sampling rate is varied from 2, 1, 1.5, and 0.5 samples per second. For each channel condition 20 readings are taken, so a total of 100 RSSI profiles from different channel conditions are used to build the RSSI profile database.

6.1.3 Vehicular Ad-hoc Networks

The rapid growth of vehicles and road-side infrastructure has given rise to vehicular networks that mainly consists of communication between vehicles and road side infrastructure. To simulate the conditions of vehicular network, we consider two cars, each equipped with laptops. The front car is equipped with the laptop Alice while the following car is equipped with the laptop. Both cars are driven simultaneously around the city, and RSSI variations are recorded. The RSSI variations are recorded for a speed of 30 km/hr.

6.1.4 Framework

To process the channel profiles, an offline key generation framework is built as shown in the Fig. 6.1. It includes:

1. MATLAB based reciprocity enhancement modules namely; l_1-norm minimisation, Hierarchical clustering, Kalman filtering, and polynomial regression.

2. MATLAB based quantisation algorithms such as; ASBG, MAQ, Radio-Telepathy, Median quantiser, ESPAR, binary quantiser, and Adaptive quantiser.

3. The IT++[89] based Turbo encoder-decoder is used for information reconciliation.

4. The secure hashes SHA-1 are derived using the open source MATLAB code provided by NIST [71].

The purpose of creating a channel profile database and an offline based framework is to allow rapid prototyping and development of key generation algorithms.

6.2 Performance Evaluation

The key generation schemes are evaluated for the set of metrics as discussed in Chapter 4 namely:

1. Bit Disagreement Rate (BDR) to evaluate the efficiency of the key generation scheme.

2. Quantization Factor (QF): Quantization factor is the percentage of bits retained after quantization. For lossless quantization, QF = 100 %, while for a lossy quantization QF $<$ 100 %.

3. Randomness test to evaluate the randomness of the generated key. The randomness test is done by using the NIST tool [71, 72].

4. Robustness test to evaluate the robustness of the method to heterogeneous channel measurements.

5. Eavesdropper test to evaluate the predictability of keys by the eavesdropper.

6.2.1 MIMO Measurements

The results of the BDR and QF are indicated in Table 6.1 and 6.2. The results indicated are averaged in each case for the following number of measurements i.e., for channel type Ch_a = 2000(200 sub-bands x 10 iterations), Ch_b = 3000(300x10), Ch_c = 2400(60x40), and Ch_d = 2400(60x40) measurements.

Table 6.1: Bit disagreement rate(%) of preliminary keys.

Channel type	Kalman filter	Polynomial regression
Ch_a	0.96	1.94
Ch_b	1.73	6.62
Ch_c	4.50	1.75
Ch_d	3.48	2.15

Table 6.2: Quantization factor(%) of preliminary keys.

Channel type	Kalman filter	Polynomial regression
Ch_a	78.60	88
Ch_b	65	73
Ch_c	78.33	87.43
Ch_d	72.64	82.67

The number of bits extracted is given by the quantization factor(QF). So considering a best case scenario, for an input of 100 bits to the quantization block, up

to 88 bits(best case for polynomial regression) and 78 bits(best case for Kalman filtering) can be extracted.

The randomness test is done by using the NIST tool. As illustrated in Table 6.3, a p value is calculated for the parameters such as: Frequency, runs, longest runs of ones, Serial, Entropy, Cumulative sums, and DFT. If ($p \geq 0.01$) for every parameter [72], then the key passes the randomness test.

Table 6.3: Evaluation of the randomness test by the NIST tool.

Criteria	Ch_a	Ch_b	Ch_c	Ch_d
Frequency	0.34	0.87	0.27	1.0
Frequency with block	0.22	0.14	0.63	0.96
Runs	0.23	0.52	0.68	0.21
Longest Runs of Ones	0.82	0.54	0.37	0.65
Serial	0.49	0.34	0.79	0.89
Entropy	0.96	0.06	0.37	0.49
Cumulative Sums	0.82	0.68	0.54	0.99
DFT	1.0	0.15	0.47	0.47

6.2.2 RSSI Profiles

Bit Disagreement and Key Generation Rates

The average BDR and KGR values for each algorithm is calculated and their performance is indicated in Table 6.4 and 6.5.

Test of Randomness

The randomness test is done by using the NIST tool. Table 6.4 indicates that all the key generation methods pass the randomness test for the RSSI profiles. The process of randomness test is illustrated in Table 6.6. For each parameter a p

Table 6.4: BDR and Randomness Test for RSSI Profiles.

Algorithm type	BDR%	Randomness Test
ASBG	24.7	Pass
Median	36.3	Pass
MAQ	32.36	Pass
ESPAR	20.6	Pass
Radio-Telepathy	37.6	Pass
Barasochhi	22	Pass
KGECR	4.5	Pass
HCKG	8.49	Pass
KFKG	6.21	Pass
CFKG	3.02	Pass

Table 6.5: KGR of RSSI profiles.

Algorithm type	Q factor	KGR (bps)
ASBG	0.45	0.9
Median	1	2
MAQ	1	2
ESPAR	0.4	0.8
Radio-Telepathy	0.175	0.35
Barasochhi	2	4
KGECR	1.705	3.41
HCKG	0.425	0.85
KFKG	1.6	3.2
CFKG	1.695	3.39

value is calculated. If $p \geq 0.01$ for every parameter [72], then the key passes the randomness test.

Eavesdropper Test

The RSSI profiles of both Eve and Janet are used to derive preliminary keys. Their BDR w.r.t Alice is calculated as indicated in Table 6.7.

Robustness test

Commercial wireless cards have a certain degree of offsets since no two wireless cards can have identical measurements. With heterogeneous channel measurements the BDR and KGR rates may get affected. To simulate the effect of heterogeneous channel measurements, artificial offsets in step of ± 5 dB is introduced ranging from -20 to + 20dB. Table 6.9 and 6.8 indicates the effect of heterogeneity on the average BDR and KGR.

6.3 Observations

The following observations are deduced from the validation and performance evaluation of key generation schemes:

1. **Testbed**: The testbed used to validate the methods of key generation consists of two types namely; wireless cards from laptops and the software defined radio USRP. The wireless cards yield real-world RSSI profiles, whereas the USRP yields real-world channel impulse response profiles.

   By using the channel impulse response profiles, magnitude and phase profiles are further derived. Hence the proposed key generation algorithms are validated using the RSSI, magnitude, and phase profiles.

2. **Frequency Selectivity**: From Fig. 6.4 we observe that the channel fading is dominant in the sub-bands from 5.15 to 5.25 GHz as compared to fading in

each individual band. Hence we choose a single RSSI value from each sub-band ranging from 5.15 to 5.25 GHz. Depending on the type of channel, the number of RSSI measurement varies per profile.

For instance, for channel Ch_a, 200 sub-bands(channels) are present, separated by 1/2 MHz and hence the RSSI profile consists of 200 values. While for the other channel conditions namely Ch_b, Ch_c, and Ch_d 300, 60, and 60 channels respectively are considered.

3. **Evaluation of RSSI Profiles**

   (a) From Table 6.4 it can be observed that the proposed algorithms namely KGECR[5], HCKG, KFKG, and CFKG[4] have decreased bit disagreement rates compared to the other methods in the state of the art. The proposed algorithms undergo enhancement in reciprocity through l_1-norm minimisation, hierarchical clustering, Kalman filtering, and curve fitting(polynomial regression).

   As a result of the enhanced reciprocity and appropriate quantisation, the bit disagreement rate is considerably reduced as compared to the other methods in the state of the art.

   (b) The KGR figures for RSSI profiles are indicated in Table 6.5.

   An increased key generation rate for KGECR, HCKG, KFKG, and CFKG methods can be observed as compared to the other methods in the state of the art. This is also due to the enhancement in reciprocity of the RSSI profile and an appropriate quantisation method thereafter.

   (c) The results of the randomness test is indicated in Table 6.4 and 6.6. Since $p \geq 0.01$ for all the parameters as shown in the table, the proposed methods pass the randomness test.

   (d) The proposed methods also pass the eavesdropper test as indicated in Table 6.7. The BDR for Eve and Janet is greater than 25% for HCKG, KFKG, and CFKG methods of key generation. Hence even

with the help of the parity bits, Eve or Janet will not be able to deduce the synchronised key. As a result the three methods are secure w.r.t passive eavesdropping.

In case of KGECR method, if Eve and Janet posses the same sensing matrix then their BDR is significantly less w.r.t to Alice. But in case Eve and Janet do not posses the same sensing matrix used by Alice and Bob, then BDR is significantly higher and hence they will not be able to predict the synchronised key.

(e) Finally the methods of HCKG, KFKG, and CFKG also pass the robustness test. In spite of a changes in the RSSI profiles due to introduction of artificial offsets, the BDR and KGR do not vary. While for the KGECR method the BDR varies and KGR does not vary.

6.4 USRP based Real-time Demonstrator

As discussed in Chapter 3, the universal serial radio peripheral(USRP) is used as a platform to validate signal processing block sets. A real-time demonstrator showing the capability of key generation in real-time is undertaken. Based on the specifications indicated in Table 6.10, signal processing blocks of the transmitter and receiver are defined in Simulink. The specification of USRP are shown in Table 6.11.

The signal processing blocks for transmitter and receiver are as shown in Fig. 6.6 and 6.8. At the transmitter, the generated binary bits are modulated by quadriphase shift keying. The modulated bits are pulse shaped using a raised cosine transmit filter with $\alpha = 0.5$ and transmitted through the USRP. The frame format consists of 26 bits of preamble (2x13 bits of Barker codes). The message bits consist of data "Hello World" numbered from (0-99). In total, the frame format consists of 200 bits including both the preamble and message bits.

At the receiver, the bits are received and corrected w.r.t their gain. After doing frequency compensation and timing recovery, the transmitted data is recovered

to display ”Hello World(0-99)”. The Simulink signal processing blocks of the transmitter and receiver are standard examples of the Simulink library. These cited standard blocks have been reused in this thesis.

Further more, the receiver block as shown in Fig. 6.8, is modified to generate keys in bi-direction. Frequency division duplexity(FDD) is used to generate the keys in bi-direction. Frequencies namely 865 MHz and 867 MHz are employed for FDD. For key generation, the RSSI is measured to obtain channel profile. The vector bits for the preliminary key are obtained by quantizing the channel profiles. For a decimation factor of 4000, the correlation co-efficient of the channel profiles in 0.8. The time taken to measure per sample is 0.2 seconds. The channel reciprocity measured in FDD mode for the frequencies 865-867 MHz is as shown in Fig. 6.9 and 6.10.

6.5 Summary

The key generation methods proposed in the previous chapter namely: KGECR, HCKG, KFKG, and CFKG are validated using testbed that reflect the real world channel measurements. The real world channel measurements include; MIMO measurements, RSSI profiles from wireless cards, and measurements obtained from the real-time demonstrator.

The channel profiles are validated using the framework as indicated in Fig. 6.1. The validation includes methods from the state of the art such as; Radio-Telepathy, ASBG, MAQ, ESPAR, Median, and Smart method of quantisation and the proposed methods namely; KGECR, HCKG, KFKG, and CFKG.

The proposed methods are validated using the following metrics namely; BDR, KGR (quantisation factor), test of randomness, robustness test, and eavesdropper test. Due to enhancements in reciprocity, the rate of disagreement between the preliminary keys is reduced as seen from Table 6.4 and 6.1. The impact of enhancing reciprocity before quantisation can also be seen in enhancing quantisation efficiency as seen in Tables 6.5 and 6.2.

Thus, a complete evaluation of the proposed methodology is presented and evaluated to validate improvements in performance of the key generation using variations of the wireless channel.

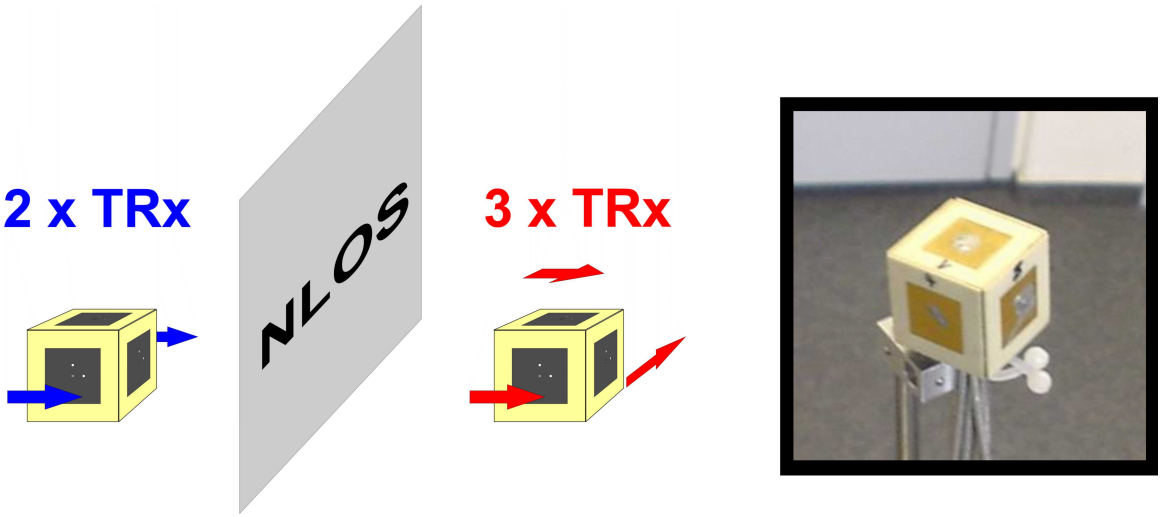

Figure 6.3: The 2x3-MIMO system was formed by antennas from two cubic antennas (left). A photograph of one antenna is shown on the right.

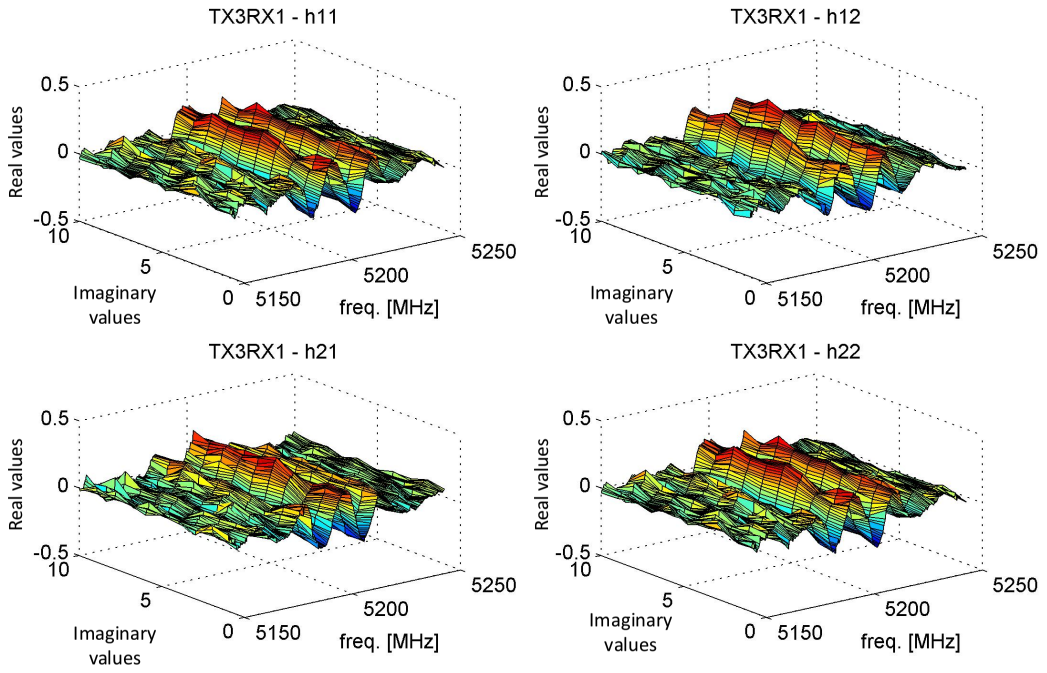

Figure 6.4: Channel estimation for channel type Ch_a. E. g., the channel matrix H for the transmission from Tx3 to Rx1 is given by H=[h11 h12 ; h21 h22]

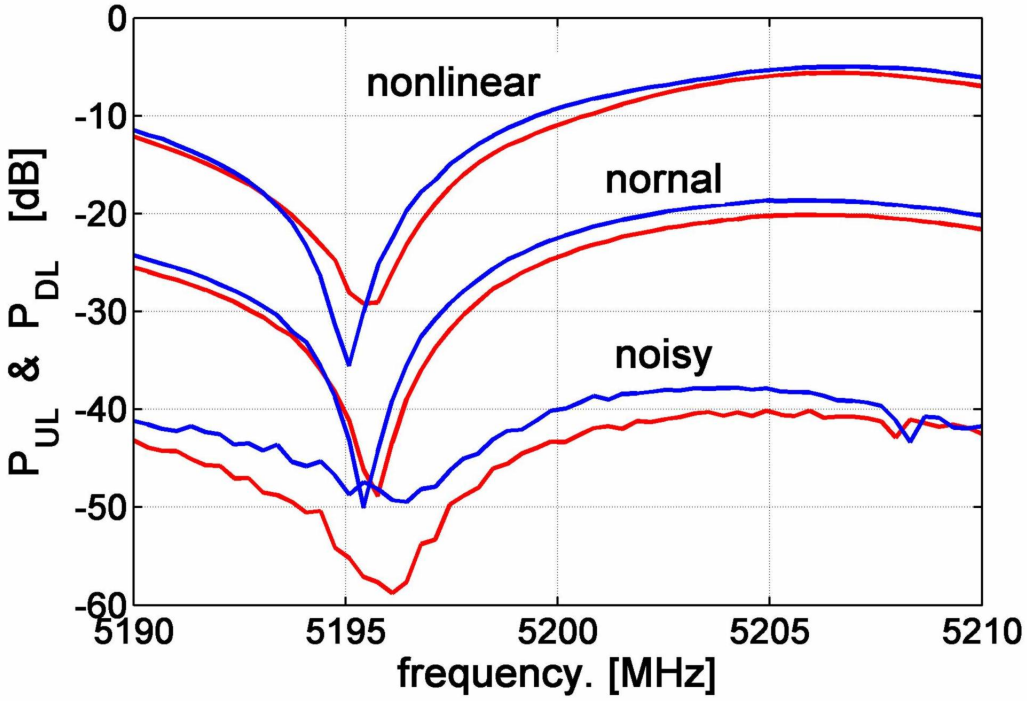

Figure 6.5: Indication of varying power levels for channel Ch_c.

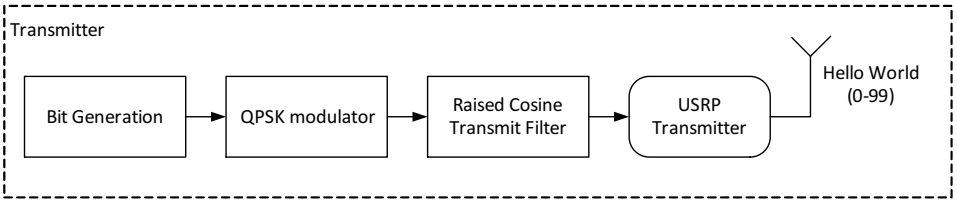

Figure 6.6: Signal processing blocks for transmitting ”Hello World”.

Table 6.6: Evaluation of the randomness test by the NIST tool.

Criteria	Indoor lab	University Campus	Cafeteria	City Center	Forest	Vehicular Channel
Frequency	0.34	0.87	0.53	0.64	0.27	1.0
Frequency with block	0.22	0.14	0.63	0.96	0.28	1.0
Runs	0.23	0.99	0.85	0.52	0.68	0.21
Longest Runs of Ones	0.71	0.48	0.82	0.54	0.37	0.65
Serial	0.49	0.34	0.79	0.89	0.65	0.52
Entropy	0.96	0.06	0.82	0.71	0.37	0.49
Cumulative Sums	0.23	0.30	0.82	0.68	0.54	0.99
DFT	1	1	0.15	0.47	0.47	0.47

Table 6.7: Eavesdropper Test on RSSI Profiles.

Algorithm type	BDR% EVE	BDR % Janet
KGECR	20.6	18.4
HCKG	59.5	52.08
KFKG	40.4	53.06
CFKG	40	46.9

Table 6.8: BDR Robustness Test on RSSI Profiles.

Algorithm type	$\pm$5dB	$\pm$10dB	$\pm$15dB	$\pm$20dB
ASBG	24.7	24.7	24.7	24.7
Median	36.3	36.3	36.3	36.3
MAQ	32.36	32.36	32.36	32.36
ESPAR	20.6	20.6	20.6	20.6
Radio-Telepathy	37.6	37.6	37.6	37.6
Barasochhi	22	22	22	22
KGECR	6.8	7.2	5.6	8.2
HCKG	8.49	8.49	8.49	8.49
KFKG	6.21	6.21	6.21	6.21
CFKG	3.02	3.02	3.02	3.02

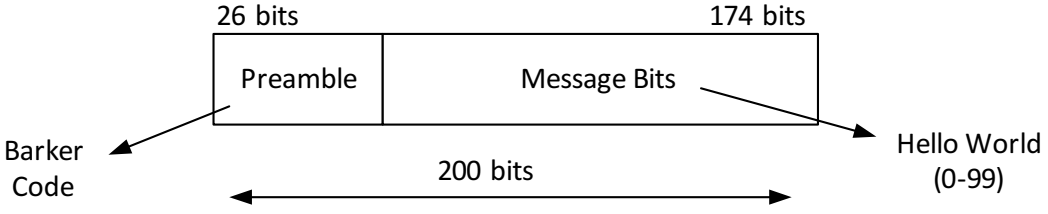

Figure 6.7: Frame format of transmitter.

Table 6.9: KGR Robustness Test on RSSI Profiles.

Algorithm type	$\pm$5dB	$\pm$10dB	$\pm$15dB	$\pm$20dB
ASBG	0.9	0.9	0.9	0.9
Median	2	2	2	2
MAQ	2	2	2	2
ESPAR	0.8	0.8	0.8	0.8
Radio-Telepathy	1.936	1.936	1.936	1.936
Barasochhi	4	4	4	4
KGECR	3.41	3.41	3.41	3.41
HCKG	0.85	0.85	0.85	0.85
KFKG	3.2	3.2	3.2	3.2
CFKG	3.02	3.02	3.02	3.02

Table 6.10: Specifications for the Signal Processing Blocks.

Parameter	Value
Modulation Scheme	QPSK
Center Frequency	f_1 = 865, f_2 = 867 MHZ
Pulse shaping	Root-raised Cosine filter $\alpha = 0.5$
Preamble	Barker codes, N=13
Scrambler	$(1, 1, 1, 0, 1)$ with $[0000]$ initial conditions
Symbol duration	$T_s = 5\mu s$

Table 6.11: Specifications of the Software Defined Radio.

Software	GNU Radio Companion
Motherboard	USRP N210
FPGA	Xilinx Spartan 3A-DSP 3400 FPGA
ADC	100 MS/s dual ADC
DAC	400 MS/s dual DAC
Connectivity	Gigabit Ethernet
Daughter board	WBX (50-2200 MHz)
Antenna	3dBi gain Vert900

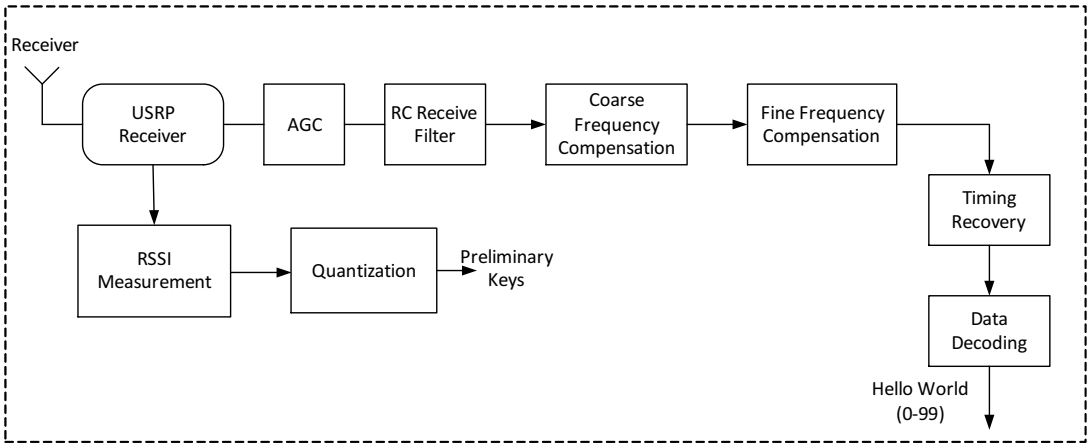

Figure 6.8: Signal processing blocks for receiver and preliminary key generation.

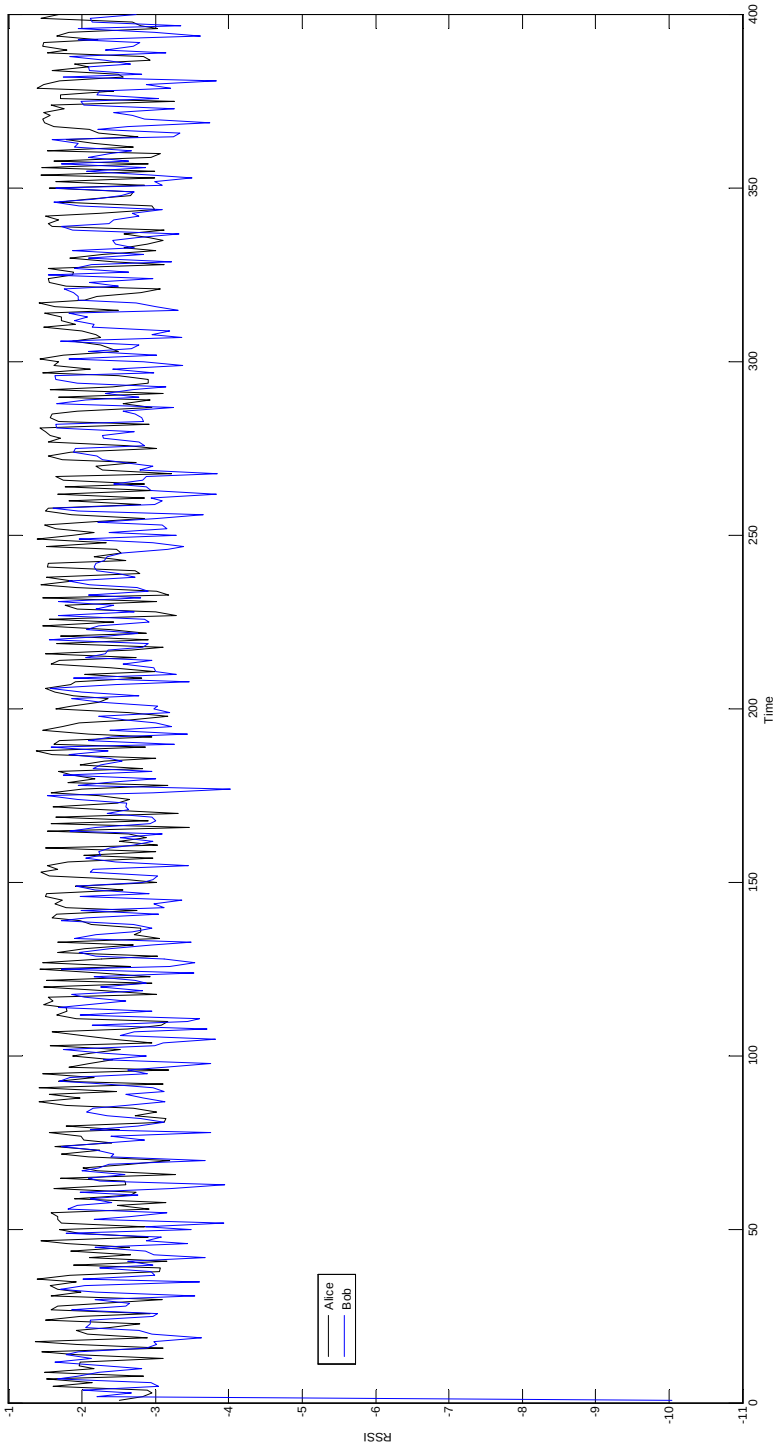

Figure 6.9: Channel reciprocity in FDD.

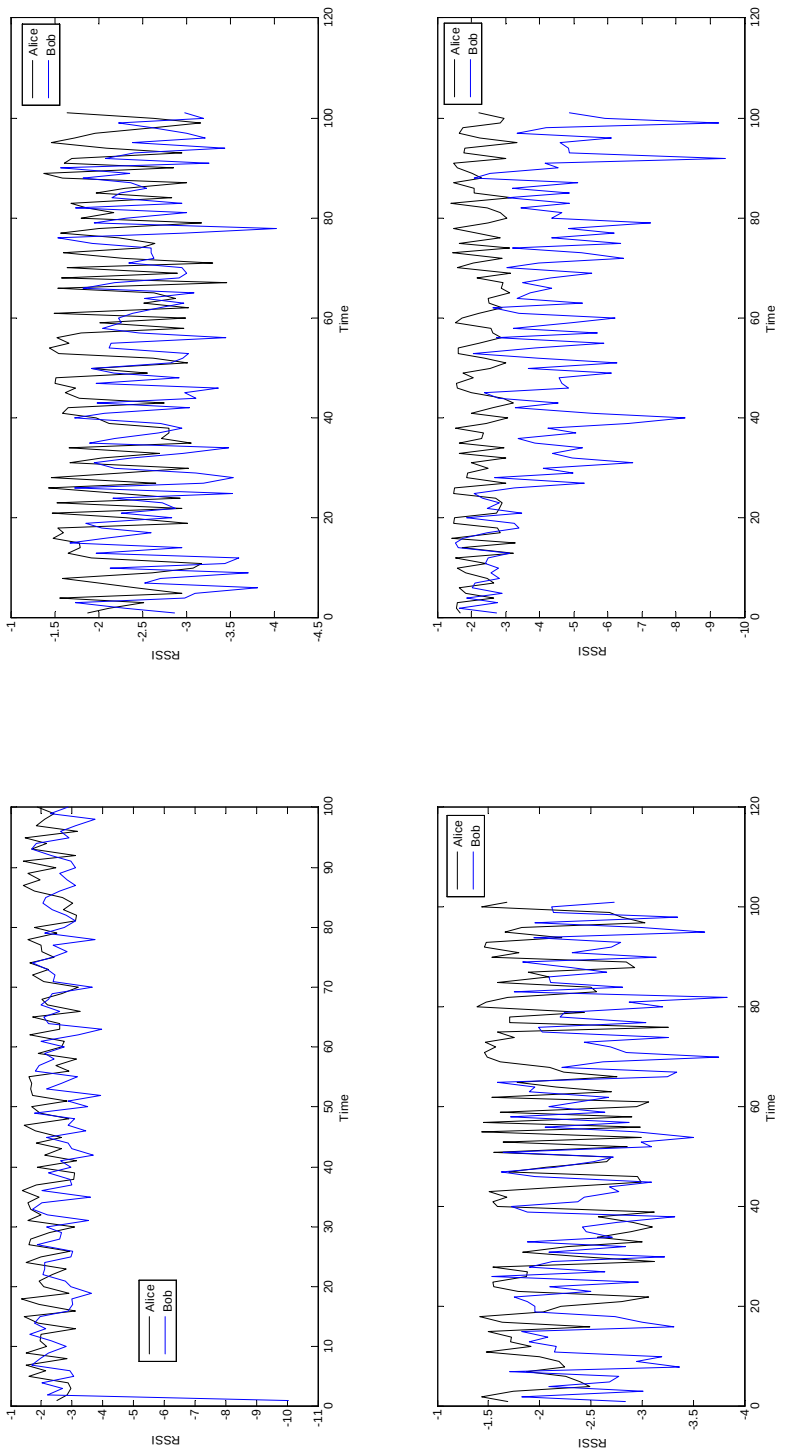

Figure 6.10: Channel reciprocity in FDD.

Chapter 7

Conclusion

7.1 Channel Aware Adaptation of Spreading Sequences

Spreading sequences are characterised by the properties of periodic and aperiodic correlation. They are usually allocated to users irrespective of their channel conditions. The principle of channel aware adaptation as described in [84] is the basis for dynamically allocating sequences to users. For a given channel condition $h(t)$, a sequence $s(t)$ is chosen such that the product of their aperiodic autocorrelation is maximised. By maximising the product, the magnitude of the energy of the received signal, is maximised and thus spreading sequences can be allocated to users based on their channel condition. Based on this principle, following are the contributions of my thesis in this topic namely:

1. By considering a simulation model, spreading sequences are allocated to users dynamically based on their channel condition. The dynamic allocation is based on an optimal allocation scheme known as the Hungarian algorithm. The performance of the down-link consisting of $K = 15$ users for Walsh-Hadamard sequences is a gain of up to 3 dB is achieved per user. While in case of Gold sequences, gain of up to 1 dB per user is achieved. The computational complexity of allocation scheme is $O(K^3)$.

2. The optimal Hungarian algorithm is computationally intensive. To combat this problem a sub-optimal but fast allocation scheme is proposed through an analytical model. The analytical model consists of a step function that allocates pseudo-dynamically instead of dynamically. A similar performance of gain up to 2 dB for Walsh-Hadamard sequences and up to 1 dB for Gold sequences is obtained at a reduced computational complexity of $O(1)$.

3. As a proof-of-concept, real-world channel estimates are obtained by using a testbed based on the software defined radio platform, USRP. The channel estimates include channel impulse responses of one, two, three and four taps. These channel estimates are used to allocate sequences to users dynamically inorder to obtain a gain of upto 1 dB for both Walsh-Hadamard and Gold spreading sequences.

Thus different methodologies for adapting spreading sequences based on the channel condition have been investigated. By choosing sequences with good cross-correlation properties and adapting these sequences based on channel conditions enhancements in the performance of the DS-CDMA downlink can be achieved.

7.2 Physical Layer Security

Fading is an inherent characteristic of the wireless channel due to which variations in the amplitude and phase of the received signal exist. By using the properties of the wireless channel, a shared secret between pair of nodes was established in [41]. The process consists of measuring the channel profile, quantizing it to get preliminary keys, detecting and correcting errors to obtain a synchronized key at both the nodes. Further methods of privacy amplification are also done to enhance system entropy.

Based on this principle, improved methods of key generation schemes utilising the random and reciprocal variations of the wireless channel have been proposed. Following are the main contributions of my thesis namely:

1. A baseline architecture model clearly depicting the four stages of key generation that have been implemented include; channel measurement, quantisation, information reconciliation, and privacy amplification.

2. A fifth stage namely *"enhancing reciprocity"* is proposed to improve the reciprocity of the channel profiles. The various methods used to enhance the channel profile are:

   (a) l_1-norm minimisation

   (b) Hierarchical clustering

   (c) Kalman filtering

   (d) Polynomial regression

3. For the l_1-nom minimisation method, a binary quantiser is used to generate the preliminary keys. While for the other three methods namely; hierarchical clustering, Kalman filtering, and Polynomial regression, an adaptive quantisation is proposed.

4. The disagreeing bits of the preliminary keys are detected and corrected using Turbo codes to obtain a synchronised keys.

5. To prevent any possibilities of key prediction, secure hash (SHA-1) of the synchronised key are generated to obtain, secure keys.

6. An architecture *KeyBunch* that utilises all the characteristic of wireless channels and generates, synchronised and secure bunch of secret keys is proposed. The main advantage of KeyBunch is that instead of generating a single key, sets of secure keys can be generated by using either the same or multiple sources of channel profile that are inturn obtained from the same physical layer.

7. As a use-case, KeyBunch is deployed in the secure vehicular communications architecture to generate keys between vehicle-to-vehicle and vehicle-to-roadside-infrastructure. By porting KeyBunch onto the HSM module it

is shown that the system entropy of the vehicular communication can be enhanced.

8. The proposed methods are validated using testbeds that reflect real world channel measurements. The real world channel measurements include; MIMO measurements, RSSI profiles from wireless cards, and USRP based real-time demonstrator.

9. Based on the metrics of BDR, KGR(quantisation factor), test of randomness, robustness test, and eavesdropper test, the proposed methods along with methods described in the state of the art are evaluated.

The evaluation results from Tables 6.1, 6.2, 6.4, and 6.5, indicate that enhancing channel reciprocity leads to a significant improvement in performance of key generation.

7.3 Future Work

The following future work is suggested as a continuation of the thesis.

1. The traditional method of designing sequences is to use mathematical tools such as Galois Fields [61] and then deduce its correlation properties. An open mathematical problem is to find sequences with known correlation properties, i.e. can a sequence be designed for any given correlation property?

2. Key generation in correlated MIMO channels: Since the channels in MIMO could be correlated, secret keys generated from such correlated sources will be weak. So it is necessary to propose methods that will extract keys from such correlated sources and yet be able to deliver improved methods of key generation.

3. Conventional methods transmit and receive using half-duplex diversity by either using Time Division or Frequency division duplexity. Recently methods of transmitting and receiving in the same frequency at the same time, i.e. full-duplex transmission and reception have been proposed in [49, 22, 23, 33]. Although still in conceptual stage, such a method offers promising prospects. Using full duplexity Alice and Bob can measure the channel profile simultaneously at the same time thereby consequently increasing the channel reciprocity and hence resulting in an improved performance of key generation.

Chapter 8

Zusammenfassung

8.1 Kanalbewusste Anpassung von Spreizcodes

Spreizcodes werden anhand ihrer periodischen und aperiodischen Korrelationseigenschaften charakterisiert. Sie werden meist Nutzern unabhängig von ihrem Kanalzustand zugewiesen. Die Grundlage von dynamischer Nutzerzuordnung ist das Prinzip der kanalbewussten Anpassung, wie in [85] beschrieben. Für einen gegebenen Kanalzustand $h(t)$ wird eine Sequenz $s(t)$ gewählt, sodass das Produkt der aperiodischen Autocorrelation maximiert wird. Die Magnitude der Energie des erhaltenen Signals wird maximiert, wenn das Produkt maximiert wird. So knnen Spreizcodes Nutzern kanalzustandabhängig zugeordnet werden. Die Hauptbeiträge meiner Arbeit sind:

1. Anhand eines Simulationsmodels werden Spreizcodes den Nutzern dynamisch und kanalabhängig zugeordnet. Die dynamische Zuordnung basiert auf dem optimalen Zuordnungsschema bekannt als Hungarian Algorithmus. Die Leistung des down-link bestehend aus $K = 15$ Nutzern verbessert sich für eine Walsh-Hadamard Sequenz um 3 dB pro Nutzer. Dagegen kann bei einer Gold Sequenz eine Leistungsverbesserung von bis zu 1 dB pro Nutzer erzielt werden. Die Komplexität für das Zuordnungsschema beträgt $O(K^3)$.

2. Der optimale Hungarian Algorithmus ist rechenintensiv. Daher wird eine suboptimale, aber schnelle, analytische Mode zur Lösung des Problems vorgeschlagen. Die analytische Methode besteht aus einer Stufenfunktion, die pseudo-dynamisch anstatt dynamisch zuordnet. Ein ähnlicher Leistungsgewinn von bis zu 2 dB für eine Walsh-Hadamard Sequenz und bis zu 1 dB für eine Gold Sequenz wird bei einer reduzierten Komplexität von $O(1)$ erzielt .

3. Als Proof-of-Concept werden Echtzeit Kanalschätzungen in einer Entwicklungsumgebung basierend auf der software defined radio platform USRP vorgenommen. Die Kanalschätzungen beinhalten Kanalimpulse von eins, zwei, drei und vier taps. Die Kanalschätzungen werden dazu genutzt Nutzern Spreizcodes dynamisch zuzuordnen, um einen Leistungsgewinn von 1 dB sowohl fr eine Walsh-Hadamard als auch für eine Gold Sequenz zu erhalten.

So wurden verschiedene Methoden für die kanalzustandsabhängige Zuordnung von Spreizcodes untersucht. Indem man Sequenzen mit guten Kreuz-korrelations eigenschaften auswählt und diese Sequenzen an den Kanalzustand anpasst, kann man die Leistung des DS-CDMA down-link verbessern.

8.2 Physical Layer Security

Abklingen (Schwund) ist eine inhärente Eigenschaft von kabelloser Übertragung, die Variationen in der Amplitude und Phase des erhaltenen Signals bewirkt. In [42] wurden die Eigenschaften von kabelloser Übertragung dazu genutzt ein geteiltes Geheimnis zwischen einem Knotenpaar auszutauschen. Der Prozess besteht aus einer Messung des Kanalprofiles, Quantisierung um einen vorläufigen Schlüssel zu erhalten, Fehlererkennung und Verbesserung um einen synchronisierten Schlüssel an beiden Knoten zu erhalten . Weiter Methoden zur Privacy Amplification werden zusätzlich benutzt um die Entropie des Systems zu verbessern.

Basierend auf diesem Prinzip wurden Methoden zur Schlüsselerzeugung, die

die zufälligen und reziproken Variationen des Kanals nutzen, vorgeschlagen. Die Hauptbeiträge meiner Arbeit sind:

1. Eine Basis Architektur, die klar die vier Phasen der Schlüsselerzeugung wiedergibt. Die vier diskutierten und umgesetzten Phase bestehen aus: Kanalmessung, Quantisierung, Information reconciliation und Privacy Amplification.

2. Eine fünfte Phase, enhancing reciprocity, wird vorgeschlagen um die Reziprozität des Kanalprofiles zu verbessern. Folgende Methoden wurden zur Verbesserung des Kanalprofils eingesetzt:

   (a) l_1-norm minimisation

   (b) Hierarchical clustering

   (c) Kalman filtering

   (d) Polynomial regression

3. Für die l_1-norm Minimierung wird die Methode des binren Quantisierens benutzt, während für die drei anderen, hierarchical clustering, Kalman filtering, polynomial regression, die adaptive Quantisierung benutzt wird.

4. Ein Architektur, KeyBunch, wird vorgeschlagen, die alle Eigenschaften eines kabellosen Kanals nutzt und einen sicheren Bund von Geheimschlüsseln erzeugt und synchronisiert. Der Hauptvorteil von KeyBunch ist, dass anstelle eines einzelnen Schlüssels ganze Gruppen von Schlüsseln erzeugt werden, die entweder die gleiche oder mehrere Quellen des Kanalprofiles nutzen und in der gleichen physikalischen Schicht entstehen.

5. Als Anwendungsbeispiel wird KeyBunch in der sicheren Fahrzeugkommunikation eingesetzt um Schlüssel zwischen vehicle-to-vehicle und vehicle-to-roadside infrastructure zu erzeugen.

6. Die vorgeschlagenen Methoden werden in Entwicklungsumgebungen, die Echtzeitkanalmessungen reflektieren, validiert. Die Echtzeitkanalmessungen beinhalten, MIMO Messungen, RSSI Profile von drahtlosen Karten und USRP basierende Echzeitdemonstratoren.

7. Basierend auf den Metriken von BDR, KGR (quantisation factor), test of randomness, robustness test und eavesdropper test werden die vorgeschlagenen Methoden mit den im State-of-Art Abschnitt beschriebenen Methoden verglichen.

Wie in den Tabellen 6.1, 6.2, 6.4 und 6.5 angedeutet, verringert der BDR die Anzahl der Fehler im vorläufigen Schlüssel, indem er die Kanal Reziprozität verbessert. Die Verbesserung der Reziprozität erhöht auch die Rate der Schlüsselerzeugung. Daraus lässt sich folgern, dass die Effizienz der Schlüsselerzeugung durch die Verarbeitung des Kanalprofiles vor der Quantiserung verbessert werden kann.

Bibliography

[1] Ericsson white paper: The future of wcdma/hspa. Technical report, February 2013.

[2] IEEE Std 802.11. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, 2012.

[3] A.A. Abidi. The path to the software-defined radio receiver. *Solid-State Circuits, IEEE Journal of*, 42(5):954 –966, may 2007.

[4] A. Ambekar, M. Hassan, and H. Schotten. Improving channel reciprocity for effective key management systems. In *Proc. of ISSSE Conference, Potsdam, Germany,*, October, 2012.

[5] A. Ambekar, N. Kuruvatti, and H. Schotten. Improved method of secret key generation based on variations in wireless channel. In *Proc. of IWSSIP Conference, Vienna*, April 2012.

[6] A. Ambekar and H. Schotten. Analysis of channel dependent adaptation of spreading sequences. In *Under submission*.

[7] A. Ambekar and H. Schotten. Keybunch: A key management architechture using physical layer security for wireless ad-hoc networks. In *Under submission*.

[8] A. Ambekar and H. Schotten. Channel dependent adaptation scheme for spreading codes in ds-cdma. In *European Wireless Conference, Lucca, Italy.*, April 2010.

[9] A. Ambekar and H. Schotten. Allocation of optimum sequences based on channel conditions in ds-cdma. In *European Wireless Conference, Vienna, Austria*, April 2011.

[10] A. Ambekar and H. Schotten. Enhancing channel reciprocity for effective key management in wireless ad-hoc networks. In *Proc. of VTC Spring Conference, Seoul, Korea,*, May, 2014.

[11] D. Anderson and P. Wintz. Analysis of a spread-spectrum multiple-access system with a hard limiter. In *IEEE Trans. on Communication Techonology*, 1969.

[12] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. *In IEEE Trans. on Antennas and Propagation.*, November 2005.

[13] M. Bala Krishna and M.N. Doja. Symmetric key management and distribution techniques in wireless ad hoc networks. In *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on*, pages 727 –731, oct. 2011.

[14] C. Berrou, A. Glavieux, and P. Thitimajshima. Near shannon limit error-correcting coding and decoding: Turbo-codes. 1. In *Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on*, volume 2, pages 1064 –1070 vol.2, may 1993.

[15] S. Beyer. Zigbee applications in sub-1 ghz frequency resuage. Presentation, November 2009.

[16] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control 3 (1)*, March 1960.

[17] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology Eurocrypt*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer Berlin / Heidelberg, 1994.

[18] E. Buracchini. The software radio concept. *Communications Magazine, IEEE*, 38(9):138 –143, sep 2000.

[19] E. Candes. Compressive sampling. In *International Congress of Mathematicians, Madrid, Spain.*, 2006.

[20] E. Candes and J. Romberg. *l1-magic: Recovery of Sparse Signals via Convex Programming*, October 2005.

[21] P. Chakraborty, A. Ambekar, and H. Schotten. Analytical model for dynamic allocation of spreading sequences in ds-cdma. In *International Symposium on Signals, Systems and Electronics, Potsdam, Germany*, October 2012.

[22] J. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving single channel, full duplex wireless communication. In *16th Annual International Conference on Mobile Computing and Networking (Mobicom)*, 2010.

[23] J. Choi, M. Jain, K. Srinivasan, R. Swensson, P. Levis, and S. Katti. A working single channel, full duplex wireless system. In *16th Annual International Conference on Mobile Computing and Networking (Mobicom)*, 2010.

[24] Tzu-Han Chou, S.C. Draper, and A.M. Sayeed. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 2518 –2522, 2010.

[25] GNU Radio Companion. http://www.joshknows.com/grc.

[26] J. Concha and S. Ulukus. Optimisation of cdma signature sequences in multipath channels.

[27] Car 2 Car Communication Consortium. http://www.car-to-car.org/.

[28] Sevecom Consortium. http://www.sevecom.org/pages/members.html, 2012.

[29] Von Altrock Constantin. *Fuzzy logic and NeuroFuzzy applications explained*. Upper Saddle River, NJ: Prentice Hall, 1995.

[30] Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin, and Adam Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 232–250. Springer Berlin / Heidelberg, 2006.

[31] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. pages 523–540. Springer-Verlag, 2004.

[32] D. Donoho and Y. Tsaig. Fast solution of l1-norm minimisation problems when the solution maybe sparse, October 2006.

[33] M. Duarte and A. Sabharwal. Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results. In *Asilomar Conference on Signals, Systems, and Computers.*, 2010.

[34] Lee Edward. Cyber physical systems: Design challenges. Technical Report Report Number UCB/EECS-2008-8, Technical report, University of California, Berkley., 2008.

[35] Pingzhi Fan and Michael Darnell. *Sequence Design for Communications Applications*. Research Studies Press LTD., 1996.

[36] Michael A. Forman and Derek Young. A generalized scheme for the creation of shared secret keys through uncorrelated reciprocal channels in multiple domains. *Computer Communications and Networks, International Conference on*, 0:1–8, 2009.

[37] R. G. Gallager. *Low Density Parity Check Codes*. Monograph, M.I.T. Press, 1963.

[38] S. Goldwasser and M. Bellare. Lecture notes on cryptography. Technical report, Summer course on cryptography, MIT., 1996-2001.

[39] H. Hartenstein and K.P. Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6):164 –171, june 2008.

[40] A. Hassan, J. Hershey, and Chennakeshu S. Apparatus and method for generating pseudorandom quantities based upon radio channel characteristics. United States Patent, Number 5995533, November 1999.

[41] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 1996.

[42] M. Hassan. Extracting secret keys from variations in wireless channel. Master's thesis, Institute for Wireless Communication and Navigation, Techincal University of Kaiserlsautern, 2012.

[43] J. Haupt, W. Bajwa, G. Raz, and R. Nowak. Toeplitz compressed sensing matrices with applications to sparse channel estimation. In *Annual Conference on Information Sciences and Systems*, 2008.

[44] J.E. Hershey, A.A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. *Communications, IEEE Transactions on*, 43(1):3 – 6, jan. 1995.

[45] Kazukuni Kobara Hideki Imai and Kirill Morozov. On the possibility of key agreement using variable directional antenna. In *1st Joint Workshop Information Security (JWIS 2006)*, 2006.

[46] H. Holma and A. Toskala. *WCDMA for UMTS - HSPA evolution and LTE*. Wiley publications, fourth edition, 2004.

[47] M. Isaka and S. Kawata. On secret key agreement from the additive white gaussian noise channel. In *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, pages 2171 – 2175, sep. 2009.

[48] iw tool. http://linuxwireless.org/en/users/documentation/iw.

[49] M. Jain, J. Choi, T. Kim, D. Bharadia, K. Srinivasan, S. Seth, P. Levis, S. Katti, and P. Sinha. Practical, real-time, full duplex wireless. In *17th Annual International Conference on Mobile Computing and Networking (Mobicom)*, 2011.

[50] William C. Jakes. *Microwave Mobile Communications*. John Wiley and Sons Inc., 1974.

[51] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proc. of MobiCom '09, Beijing, China*, 2009.

[52] V. Jungnickel, U. Krueger, G. Istoc, T. Haustein, and C. von Helmolt. A MIMO system with reciprocal transceivers for the time-division duplex mode. In *Proc. IEEE Int. Symp. Antennas and Propagation*, Monterrey, CA, June 2005.

[53] Bhavana Kanukurthi and Leonid Reyzin. Key agreement from close secrets over unsecured channels. In Antoine Joux, editor, *Advances in Cryptology*

- *EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 206–223. Springer Berlin / Heidelberg, 2009.

[54] S. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall, 1998.

[55] Akito Kitaura and Hideichi Sasaoka. A scheme of private key agreement based on the channel characteristics in ofdm land mobile radio. In *Electronics and Communications in Japan*, volume 88, 2005.

[56] Donald Knuth. *The Art of Computer Programming, volume 3, Sorting and Searching*. Addison-Wesley,, 1998.

[57] H. Koorapaty, A.A. Hassan, and S. Chennakeshu. Secure information transmission for mobile radio. *Communications Letters, IEEE*, 4(2):52–55, feb. 2000.

[58] N. Kuruvatti. Extracting secret keys from variations in wireless channel. Master's thesis, Institute for Wireless Communication and Navigation, Techincal University of Kaiserlsautern, 2012.

[59] Charan Langton. Coding and decoding with convolutional codes. Internet link: http://complextoreal.com/chapters/convo.pdf.

[60] Junyi Li, M. Wodczak, Xinzhou Wu, and T.R. Hsing. Vehicular networks and applications: Challenges, requirements and service opportunities. In *Computing, Networking and Communications (ICNC), 2012 International Conference on*, pages 660 –664, 30 2012-feb. 2 2012.

[61] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 2002.

[62] Masoud Ghoreishi Madiseh. Secret key generation and agreement in uwb communication channels. Master's thesis, Department of Electrical and Computer Engineering, University of Victoria., 2008.

[63] M.G. Madiseh, M.L. McGuire, S.S. Neville, Lin Cai, and M. Horie. Secret key generation and agreement in uwb communication channels. pages 1 –5, nov. 2008.

[64] M.G. Madiseh, M.L. McGuire, S.W. Neville, and A.A.B. Shirazi. Secret key extraction in ultra wideband channels for unsynchronized radios. pages 88 –95, may. 2008.

[65] S. Mathur, M. Narayan, Y. Chunxuan, and A. Reznik. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proc. of MobiCom '08, San Francisco, USA.*, 2008.

[66] Ersin Uzun Matthias Wilhelm, Ivan Martinovic and Jens Schmitt. Sudoku: Secure and usable deployment of keys on wireless sensors. In *6th Annual Workshop on Secure Network Protocols(NPSec)*, 2010.

[67] Ivan Martinovic Matthias Wilhelm and Jens Schmitt. Key generation in wireless sensor networks based on frequency-selective channels: Design, implementation and analysis. Technical report, arXiv:1005.0712v1 [cs.CR]. ArXiv.org,, 2010.

[68] Ueli Maurer. A universal statistical test for random bit generators. *Journal of cryptology*, 5:89–105, 1992.

[69] J. Mitola. The software radio architecture. *Communications Magazine, IEEE*, 33(5):26 –38, may 1995.

[70] Gordon Moore. Cramming more components onto integrated circuits. Electronics Magazine, 1965.

[71] NIST. http://csrc.nist.gov/groups/st/toolkit/rng/documentationsoftware.html.

[72] NIST. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, 2001.

[73] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communcations Magazine*, 46(11):100–109, November 2008.

[74] N. Patwari, J. Croft, S. Jana, and S.K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *In IEEE Transactions on Mobile Computing,*, 9(1):17 –30, jan. 2010.

[75] W.W. Peterson and D.T. Brown. Cyclic codes for error detection. *Proceedings of the IRE*, 49(1):228 –235, jan. 1961.

[76] Sriram Nandha Premnath, Sneha K. Kasera, and Neal Patwari. Secret key extraction in mimo-like sensor networks using wireless signal strength. *SIGMOBILE Mob. Comput. Commun. Rev.*, 14(1):7–9, 2010.

[77] M. Pukkila. Channel estimation modelling. Technical report, Post-graduate Course in Radio Communications, Nokia Research Center, 2000.

[78] Kui Ren Qian Wang, Hai Su and Kwangjo Kim. Fast and scalable secret key generation exploiting channel phase randomness in wireless netwotrks. Undr submission.

[79] M. Dell"Amico R. Burkard and S. Martello. Assignment problems. SIAM.

[80] GNU Radio. http://gnuradio.org/.

[81] M. Rupf and J. Massey. Optimum sequence multisets for synchronous code-division multiple-access channels. In *IEEE Trans. on Information Theory*, July 1994.

[82] B. Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In *Proc. of CCS '07*, 2007.

[83] D. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences (corresp.). *Information Theory, IEEE Transactions on*, 25(6):720 –724, november 1979.

[84] H. Schotten. Method and system for adapting an effective spreading sequence in a communication system using direct sequence spreading. United States Patent, Pub.No.: US 2006/0285524 A1, Pub. Date: Dec. 21, 2006.

[85] T. Shimizu, N. Otani, T. Kitano, H. Iwai, and H. Sasaoka. Experimental validation of wireless secret key argeement using array antennas. In *Graduate Shool of Engineering,*, Kyoto.

[86] V.M. Sidelnikov. On mutual correlation of sequences. In *Soviet Math Doklady*, 1971.

[87] H. Sun, V. De Florio, N. Gui, and C. Blondia. Promises and challenges of ambient assisted living systems. In *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*, pages 1201 –1207, april 2009.

[88] Hisato Iwai Takayuki Shimizu and Hideichi Sasaoka. Improvement of key agreement scheme using espar antenna. In *International Symposium on Antennas and Wave Propogation*, 2008.

[89] IT++ tool. http://itpp.sourceforge.net/stable/.

[90] David Tse and Pramod Vishwanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 1995.

[91] Sennur Ulukus. *Power Control, Multiuser Detection and Interference Avoidance in CDMA Systems*. PhD thesis, Graduate School - New Brunswick, Rutgers, The State University of New Jersey, 1998.

[92] P. Vishwanath and V. Anantharam. Optimal sequences and sum capacity of synchronous cdma systems. In *IEEE Trans. Info. Theory*, September 1999.

[93] P. Vishwanath, V. Anantharam, and D. Tse. Optimal sequences, power control and capacity of spread-spectrum systems with multi-user receivers. In *IEEE Trans. on Information Theory*, September 1999.

[94] J.W. Wallace, Chan Chen, and M.A. Jensen. Key generation exploiting mimo channel evolution: Algorithms and theoretical limits. pages 1499 –1503, mar. 2009.

[95] G. Welch and Bishop G. An introduction to the kalman filter. Technical report, University of North Carolina at Chapel Hill, July, 2006.

[96] R. Welch. Lower bounds on the maximum cross correlation of signals. In *IEEE Trans. on Information Theory*, May 1974.

[97] Hong Wen and Guang Gong. A cross-layer approach to enhance the security of wireless networks based on mimo. In *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, pages 935 – 939, mar. 2009.

[98] M. Wilhelm, I. Martinovic, and J.B. Schmitt. On key agreement in wireless sensor networks based on radio transmission properties. In *Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on*, pages 37 –42, 2009.

[99] Matthias. Wilhelm, Ivan. Martinovic, and Jens Schmitt. Light-weight key generation based on physical properties of wireless channels. In *11. Kryptotag der Gessellschaft für Informatik e.V., page 4, University of Trier, Germany.*, 2009.

[100] Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt. Secret keys from entangled sensor motes: implementation and analysis. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 139–144, New York, NY, USA, 2010. ACM.

[101] J. Winkley, P. Jiang, and W. Jiang. Verity: An ambient assisted living platform. *Consumer Electronics, IEEE Transactions on*, 58(2):364 –373, may 2012.

[102] Chunxuan Ye, A. Reznik, and Y. Shah. Extracting secrecy from jointly gaussian random variables. pages 2593 –2597, jul. 2006.

[103] Kai Zeng, D. Wu, An Chan, and P. Mohapatra. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In *Proc. of INFOCOM, 2010 Proceedings IEEE*, mar. 2010.

[104] C. Zenger, A. Ambekar, F. Winzer, T. Poeppelmann, H. Schotten, and C. Paar. Preventing scaling of successful attacks: A cross-layer security architechture for resource-constrained platforms. In *Proc. of International Conference on Cryptography and inforamtion Security - BalkanCryptSec*, 2014.

[105] L. Zhou and Z. Haas. Securing ad-hoc networks. *IEEE Networks*, November 1999.

CURRICULUM VITAE

ABHIJIT AMBEKAR

EDUCATION

Master of Technology(M.Tech) July 2008
International Institute of Information Technology, Bangalore, India.

Bachelor of Engineering(B.E.) June 2006
Visvesvaraya Technological University, Belgaum, India.

EXPERIENCE

DFKI Kaiserslautern 2015-present
Researcher, Intelligente Netze

Techincal University of Kasierslautern 2009-2015
Research Associate
Chair for Wireless Communications and Navigation
Doctoral thesis: Exploiting radio channel aware physical layer concepts.